LAUREA

Public Key Infrastructure operations model

Ruohomäki, Petteri

2012 Leppävaara

Laurea University of Applied Sciences
Espoo Institute

Public Key Infrastructure operations model

Petteri Ruohomäki
Information Systems
Thesis
May 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Suuntautumisvaihtoehto

Petteri Ruohomäki

Public Key Infrastructure operations model

Vuosi 2012 Sivumäärä 64

Opinnäytetyö on jaettu kahteen osaan. Ensimmäinen osa on julkisen avaimen infrastruktuuri toimintamallin esittely ja toinen on toimintamallin arviointi. Opinnäytetyö vastaa kysymykseen, kuinka yritys pystyy tarjoamaan tehokkaamman ja johdonmukaisemman julkisen avaimen infrastruktuurin. Keskeinen kysymys on, kuinka yritys pystyy tunnistamaan vastapuolen turvallisesti. Yrityksellä tulee olla luottamus syötteisiin.

Toimintamalli on rakennuttu perustuen Information Security Forumin parhaisiin käytänteisiin. Toimintamalli on rakennettu finanssialan yrityksen tarpeisiin. Finanssiala on eniten säännöksiä omaavampia aloja ja vaatimukset ovat kovia. Korkeiden kriteereiden vuoksi mallin implementointi tulisi olla mahdollista myös muille toimialoille. Toimintamalli on rakennettu perustuen useisiin standardeihin ja parhaisiin käytänteisiin.

Arviointiosio perustuu finanssialan Julkisen avaimen infrastruktuuri -projektiin. Projekti on osaprojekti Yhtenäinen euromaksualueen muutos -projektista. Julkisen avaimen infrastruktuuri -projekti kestää yli kolme vuotta ja se hyödyntää kaikkia toimintamallin osa-alueita. Tämän takia malliprojekti on optimaalinen arvioimaan Julkisen avaimen infrastruktuuri -toimintamallia. Mallin arvioinnin tulisi vastata kysymykseen, onko toimintamalli hyödynnettävissä ja voidaanko toimintamalli implementoida muihin ympäristöihin?

Opinnäytetyössä käytetään suunnittelututkimuksen metodia. Suunnittelututkimuksella on kaksi aktiviteettiä: rakenna ja arvioi. Ilmentymä rakennetaan, koska halutaan kuvata miten se oikeasti toimii. Opinnäytetyön ilmentymä on Julkisen avaimen infrastruktuuri -toimintamalli. Rakentaminen on prosessi, jolla luodaan ilmentymä tiettyyn tarkoitukseen. Arviointi on prosessi, joka tarkastelee, miten hyvin ilmentymä toimii. Arvioinnin kriteerit pitää määritellä. Ilmentymän rakennusvaiheessa toimintaa ei välttämättä vielä ymmärretä kovin hyvin, vaan vasta arviointivaiheessa voidaan saada selkeä kuva tutkittavasta aiheesta.

Opinnäytetyön tuloksista on kehitetty ilmentymä Julkisen avaimen infrastruktuuri -toimintamallista. Tämä toimintamalli antaa ensimmäiset askeleet siitä, mitä tulee tehdä Julkisen avaimen infrastruktuuri -projektissa. Tämä toimintamalli antaa osittain vastauksia kysymykseen, kuinka kehittää tehokkaammin, halvemmin ja turvallisemmin Julkisen avaimen infrastruktuuri -palveluita. Tulokset ovat oikeasta julkisen avaimen infrastruktuuri projektista ja ne ovat vertailtavissa muihin projekteihin.

Asiasanat: Julkisen avaimen infrastruktuuri, PKI, Toimintamalli

Laurea-university of Applied Sciences **Abstract**
Laurea Leppävaara
Information Technology Program
Information Systems and Data Communication

Petteri Ruohomäki

Public Key Infrastructure operations model

Year 2012 Pages 64

My thesis is divided in two parts. The first part deals with the Public Key Infrastructure operations model and the second offers an evaluation of that model. The thesis answers how to provide efficiency and consistent Public Key Infrastructure functionality to a company. The main question is how a company can identify the counterparty player securely. A company must be able to trust outputs and inputs.

The model is based on Information Security Forum best practices and it is built for the companies in the financial sector. Being one of the most regulated sectors, the requirements are set high. This is the reason why the model should have possibilities for easy implementation implement to other environments. Model built on multiple standards and best practices.

The evaluation phase is grounded on the financial sector Public Key Infrastructure project. This project is part of Single Euro Payments Area financial changes. The project length exceeds three years, and it uses all model phases. For this reason the company Public Key Infrastructure project is optimal for evaluating the Public Key Infrastructure operations model. Model evaluating should answer on whether the model is usable and it be implemented to other environments.

This thesis relies on the Design research method, the final product being the Public Key Infrastructure operations model. Design science contains two principle activities: build and evaluate. Building the artifact demonstrates how it works. In this study building means the process of constructing the actual artifact, the Public Key Infrastructure operations model. Evaluation, for its part, is the process of terming how well the artifact works. Specific criteria must be set up for successful evaluation. This mean that when to build artifact as Public Key Infrastructure operations model so functioning may not be well understood.

The thesis result is the artifact of Public Key Infrastructure operations model. This model offers the first steps on what must be done in the Public Key Infrastructure project. It provides a partial answer on how to develop faster, more efficient, and safer Public Key Infrastructure services. The thesis results are derived from a real Public Key Infrastructure project, but these kinds of projects are comparable with one another.

Key words: Public Key Infrastructure, PKI, Operations model

Abbreviations used on this thesis

ACLs	Access Control Lists
AIA	the Authority Information Access
AUK	Authentication Key
CA	Certificate Authority
CDP	CRL distribution point
CKMS	Cryptographic Key Management Systems
COBIT	Control OBjectives for IT
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate revocation list
DES	Data Encryption Standard
EPC	the European Payments Council
HSK	the Hashing Key
IETF	the Internet Engineering Task Force
ITIL	Information Technology Infrastructure Library
IPsec	Internet Protocol Security
ISACA	Information System Audit and Control Association
ISF	Information Security Forum
ISO	International Organization for Standardization
KEK	Key Exchange Key
LDAP	Lightweight Directory Access Protocol
PCI	Payment Card Industry
PKI	Public Key Infrastructure
PMBOK	Project Management Body of Knowledge
PRINCE2	Project IN Controlled Environment
RA	Registration authority
RFO	Request for Order
RFP	Request for Proposal
S/MIME	Secure/Multipurpose Internet Mail Extensions
SEPA	Single Euro Payments Area
SSL	Secure Socket Layer
TLS	Transport Protocol Security

Index

1 Introduction

This thesis is a review of public key infrastructure operations model. The thesis discussion begins from business needs and ends with support and maintenance. It asks what users should take into consideration in the public key infrastructure project? Thesis model is build to a financial company and that model is based on known security forum solution. Thesis result is evaluated public key infrastructure model. Thesis knowledge base is known reliable sources and company own PKI project lesson and learns results. Thesis uses a design science research method.

Confidentiality, integrity, availability and non-repudiation are what companies want for services. PKI (public key infrastructure) offers one solution. PKI is based on trust. All parties must be able trust each other. Most common way to use PKI is internet browsers certificates user or service identification certifications. As such PKI is not a new solution to the secure networks and users. The first finding of secure communications messages dates back to year 1949. Shannon defines the need as "secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal." (1949. 1). Later, in 1973, Feistel noted that computer lines are open to corruption of traffic. Therefore, data secrecy must provide adequate protection against operational deception of the system. (1973. 1)

PKI can be used in all situations where confidentiality, integrity, availability and non-repudiation services are needed. It is applicable for securing VPN (Virtual Private Network) connections or identifying the system user. Other solutions include web security like server authentication or client authentication. One of the user applications is email encrypting. This means that sharing digital signatures so that mails have confidentiality between messages. PKI can be use also to encrypt file systems. Smart card authentication is normally bases on PKI environment. These are used for web applications and operate system authentications. One of the consumer services in Finland is the mobile certificate. The Finnish mobile certificate is an electronic identification document that the user can exploit in a mobile phone. The personal certificate is built-in in the SIM (Subscriber Identity Module) card. (Mobile certificate 2011.) An older, yet widely used, solution is the TUPAS (Identification Service for Service Providers). Banks identify their customers by applying the same bank-specific identifiers that the customer uses in the bank's individual services. The TUPAS service is typically used in Internet services. TUPAS as such is not directly related to this thesis, but it is a common system in the financial sector (Federation of Finnish Financial Services. 2011. 4)

PKI is used frequently in different environments. Because of its common use criminal elements have shown plenty of interest toward it. Normally this is noticed in identity thefts. PKI service providers also qualify as criminal targets because of their active use. Latest criminal acts include the RSA (Coviello 2011), compromised Diginor certificates (Interim Report 2011) and Beast, where transport layer security was compromised (Cert-fi). Cases are more prepared and pointed to certain system or environment. Case Comodo is an example for that. "The attacker was well prepared and knew in advance what he was to try to achieve. He seemed to have a list of targets that he knew he wanted to obtain certificates for, was able quickly to generate the CSRs for these certificates and submit the orders to our system so that the certificates would be produced and made available to him." (Comodo incident report 2011) In 2012 the world's largest SSL (secure socket layer) certificate issuing authority Verisign faced several successful attacks against its corporate network. The purpose of the attacks was to access computers and servers and to get secure information. (Keizer, B. 2012.)

Authorities and governments grant standards, best practices and laws telling what companies should do? Best known standards or best practices are the NIST (National Institute of Standards and Technology), ISO (International Organization for Standardization), ITIL (Information Technology Infrastructure Library), COBIT (Control OBjectives for IT) and PCI (payment card industry). The Owner of the PCI standard is PCI Security Standards Council. At least PCI standards have two different areas where to use PKI. In the first one all sensitive information must be encrypted during transmission over networks (PCI Security Standards Council LLC. 2010.35). Second is to make sure that all persons have unique identification (PCI Security Standards Council LLC. 2008.46). Companies are required to use standards and best practices in the contract level. Laws HIPAA (the Health Insurance Portability and Accountability Act) and SOX (the Sarbanes-Oxley Act) define how to use authentication like PKI.

Finnish government money laundry act sets requirements to financial companies. Acts define that the company must identify the customer's identity with strong authentication (Ministry of the Interior. 2008). Act on Electronic Signatures defines "the operations of a certification service provider providing qualified certificates to the public shall be careful, reliable and appropriate and non-discriminatory towards its customers. The certification service provider shall have technical expertise and financial resources sufficient vis-á-vis the scope of operations. The certification service provider shall be liable for all aspects of the certification operations, including the reliability and functionality of any services and products produced by parties assisting the certification service provider." (Ministry of the Interior. 2003)

2 Research Problem

My main research problems deal with the following dilemmas: what a user should take into consideration in a public key infrastructure project and how to make sure that the company has a secure, efficient, and consistent PKI solution. Companies have started to use PKI solutions in several environments. Confidentiality, integrity, availability and non-repudiation are the principal concerns in the banking or healthcare environment. The question is how to satisfy business demands? How companies can be sure of the reliability of the counterparty player? How any company employer can be sure where the mail comes from without a reliable certification? There has to exist some way how to trust intercompany connections and mails?

The financial sector started using data communication connections around 1980. Now almost all communication between customers and financial companies takes place by using data communication. Data communication means bank cash machines, bank to bank communication, bank to customer connections, or different payment channels like e-invoice. Bank to bank communication operates in closed Swift network. (Kontkanen 2008. 187) The development in financial payments sector has been very active in recent years because of SEPA (Single Euro Payments Area). This new development has changed some of the quintessential payment channels and the overall operational structures. There are these days more rules and more banks in critical clearing cycles. SEPA has also changed data transfer methods and encryption issues.

The main concern is how to provide a systematic progression to handle all PKI project factors. In some cases it is important that all factors are processed. A telling example is that a company builds their own infrastructure but they do not check their own certification usability. In the Cross certification cases counterparty policy set usability to company certifications. These include well known public services like VeriSign. That is one of the reasons why cross certification research work must be done.

Outsourcing is another case. Companies must investigate what kinds of regulators are involved in the use PKI environment. For example, some laws must be followed, or there might exist some national regulators like Federation of Finnish Financial Services. There is a worldwide service provider VISA. VISA drive companies to use PCI Security Standards Council standard. Large companies might have their own policy what must be followed.

Common PKI environments are typically audited regularly or annually. There are a number of auditing guides that describe the PKI rules a company should follow. Finnish national security auditing criteria reads that “Secret keys are only in use for authorized users and processes. Processes and procedures for key management are documented and appropriately imple-

mented." (Ministry of Defence. 2011. 88). Another audit framework is the COBIT (Control OBjectives for IT). COBIT define in DS5 (deliver and support phase 5) security cryptographic key management as follows: "Determine that policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure." (The IT Governance Institute. 2001. 118)

The European Commission outlines that internet users must be safe and secure when they connect online. In EC's thinking it is as if the user was functioning in the physical world. Cybercrime cannot be tolerated. Electronic banking or Health would not exist if new technologies proved unreliable. The world, however, is experiencing a growing epidemic in identity theft and online fraud. Attacks are becoming increasingly sophisticated and often motivated by financial or political purposes. (European Commission. 2010. 16)

Every project has a definite beginning and a definite end (PMBOK guide 2004. 5). It is vital that there exists a timetable for when the PKI environment must be ready. Normally the PKI environment is part of some large project. For example, when a company adds a new connection to the new environment by Web service to save connection and file transfer, it needs a working PKI environment. A PKI project contains numerous vital stages, like the technique and the corporate stage. Technique stage involves building up the environment, while the corporate stage deals more with handling agreements and certificate policies between the individual company, customer, and PKI environment provider. As they progress, the projects typically outline improved processes. In some cases new process development starts before the actual project has even ended.

The project opportunity window is usually temporary (PMBOK guide 2004. 6). A PKI project must use this. Afterwards it is more difficult to get funding and resources to the development of the project. PKI environment is normally part of larger development project. It is quite commonplace that the company that owns the project does not have PKI knowledge. That is the main reason why it should use outside knowledge. The question is how a company can follow what must be done without the necessary knowledge. For these cases a company needs a model list of best practices to follow.

A Guide to the project management body of knowledge defines that project activities cannot be normal activities (2004. 7). Guide also defines strategic considerations (2004. 7):

- Market demand
- Organizational need
- Customer request
- Technological advance
- legal requirements

There could be a future market demand for PKI in mobile certification for the private customers. An example for Organizational need PKI could be the need to provide secure transmissions between own and outsourced systems. Corporate customer PKI requests could be policy requirements for transmissions between customers to the company. In some cases technological advance gives the company more secure or easier way to provide PKI environment services to customers or company's own processes. Governments or commercial authorities like the PCI actor force the company to use a specific PKI solution so the company can operate within the parameters of laws and regulations.

Information security projects like the PKI project typically establish new technologies and processes. In selecting new technologies there exists a need for wide scale experience so all the aspects are valid. Latest but unknown the solution is not attractive to the project group. The company personnel require specific training when facing a new subject. This increases the risk of human resources turnover because new skills might be desired in other companies. (Mattord & Whitman 2010. 20)

Factors what must be solved in the PKI project:

- Requirements
- Infrastructure
- Trust model and cross certification
- Standards
- Scalability
- Performance and offline behavior
- Technology decision
- Outsourcing
- Security

2.1 Project

My thesis focuses on the financial sector operational environment, which is one of the most regulated professional sectors with high requirements. This PKI model is based on identified financial sector requirements. It focuses specifically on banking and on one of the core services in the banking sector, financial transmission (Kontkanen 2008. 12). Transmissions take place between banks or customers. Customers are corporate customers.

The reference project is related to the financial sector data transfers. Situation was that a financial company needed a new channel with PKI verification. The channel solution was new so all PKI work began as a business case. This was an optimal project for this thesis because it uses all steps of the operations model. PKI solution is replacing old PATU model. The PATU security model is the base on the DES (Data Encryption Standard) keys. Three keys in use are the HSK (The Hashing Key), AUK (The Authentication Key) and KEK (The Key Exchange Key). Transmission parties share their own copies of the keys. The customer must set keys for each bank, and the bank must set keys for each of its customers. (The Finnish bankers' association - Information security committee 2001. 6)

The project requirements for the PKI part were defined by a coalition of financial companies. Specifications defined that the PKI must use a X.509v3 standard certification. Certification is used for two logically different purposes. First: to authenticate the party that generated the signed data. Second: to ensure that the signed data has not been modified in transit. Specification excludes PKI generation, distribution, administration and use. (Nordea, OP-Pohjola Group, Sampo Bank 2008)

This project is part of larger financial payment transformation which has started from the SEPA (Single Euro Payments Area) changes. Citizens of the European Union can make payments in 32 countries using the same specification to build up transactions. The European Payments Council (EPC) defines the SEPA payment schemes and frameworks. EPC has an impact on security requirements. (European Payments Council. SEPA visions and goals)

2.2 Public key infrastructure

In 1976 Diffie, Hellman and Merkle developed public key cryptography, next year Rivest, Shamir and Adleman conceived the RSA algorithm, while the year after that Lohnfelder invented the certificate. Latest specification of certifications dates to 1999 when Internet PKI certificate and CRL (certificate revocation list) profile RFC2459 (Request for Comments) and Internet PKI certificate policy and certification practices framework RFC2527 IETF (The Internet Engineering Task Force) documents were published. (Housley, R & Polk, T. 2001. 2)

Components of the PKI are CA (Certification Authority), CRL (Certificate revocation list), Repository, RA (Registration authority), and archive and Infrastructure users. The CA represents a combination of computer hardware, software and operative users. First CA function is to create and sign certificates. Second is to maintain certificate status information. Next is to publish current certifications and CRLs. Fourth, and the final one, is to maintain archives status. (Housley, R & Polk, T. 2001. 44)

The CA can issue certificates to users or other CAs. When CA issues certificate it issues public and private corresponds. The CA inserts name to certification so users can easily identify it. Users verify signature by using CA's public key to ensure that the certification is valid. Private Key tells CA name and after verification trusts that private key. This is the reason why the user must protect the private key. (Housley, R & Polk, T. 2001. 45)
The CA must update CLR list so certifications statuses are updated. Protecting these statuses is similar to protecting the certificate profile. The CA is only useful when the certificates and CRL lists generates are available to the users. The CA certification and CRL are public so there is no security issue when CA publishes these. Only the private key must be secured. The CA must maintain information so as to identify the signer of an old document based on an expired document. Also revocation information must include that information. CA can build up audit trail of all actions so all known steps are easier to follow. This is a common attribute but not usually used. (Housley, R & Polk, T. 2001. 46)

The image below demonstrates the relationship between entities defined in terms of the PKI management processes. The letters point out PKI management messages. (Adams C. & Farrell S. 1999. 5)

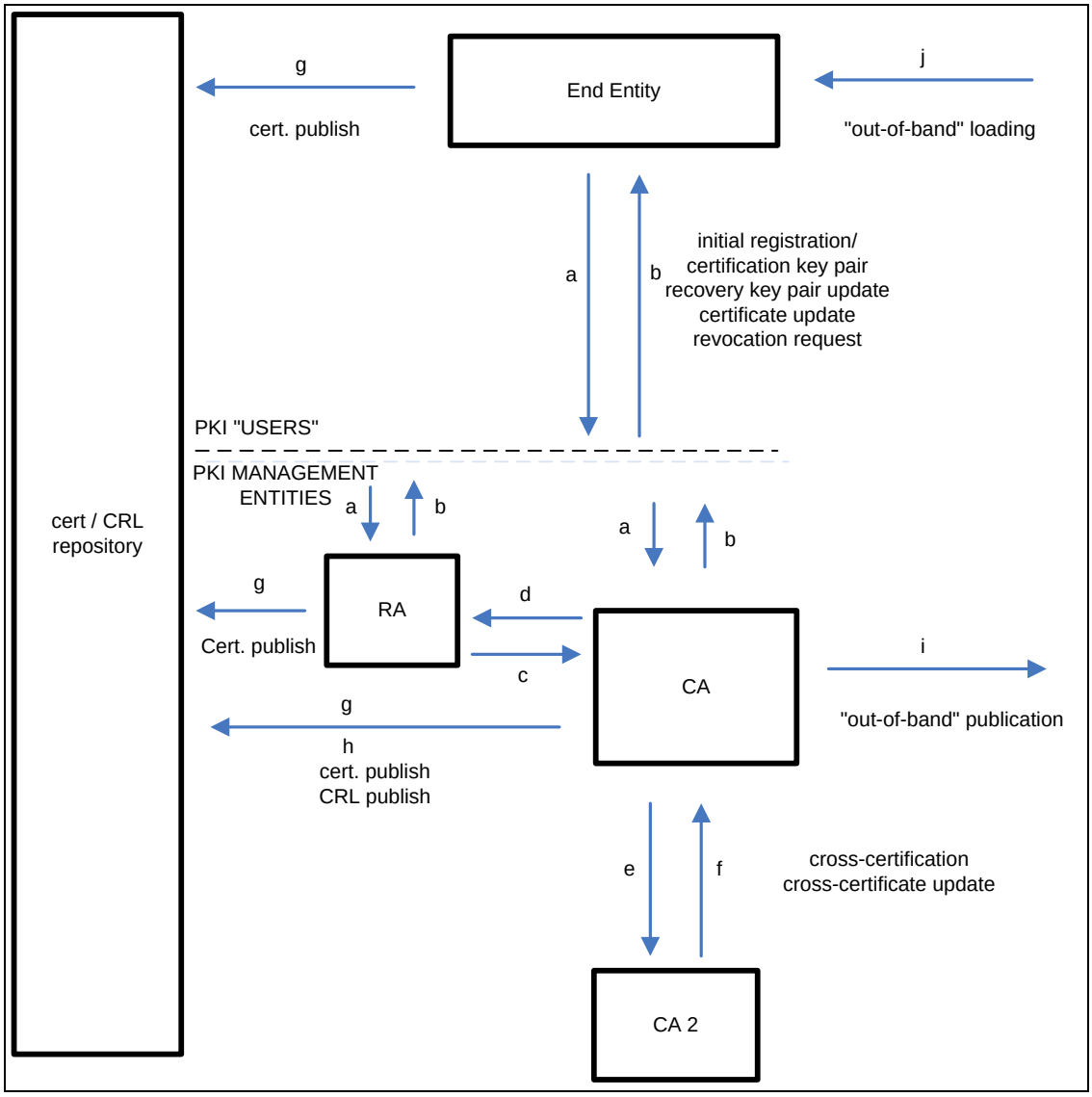


Figure 1 PKI Certificate Management Protocols
(Adams C. & Farrell S. 1999. 6)

The main purpose of the RA is to verify certificate content for the CA. The RA functions as a link between the customer and the CA and performs information verifications before the first key par is transferred to the customer. In some cases the RA can publish certifications by itself if they have access to the CA environment. A Repository system distributes certificates and CRLs. A repository accepts certificates and CRLs from CAs to several different security services. Archive is responsible for long term CA information storage. Data is loaded to archive but after that archive data remains static. (Housley, R & Polk, T. 2001. 49)

There are three different solutions for PKI architecture. First is simple architecture. The simple architecture is straightforward. There is one trusted CA and one CRL for certification validation. There can be several certifications. There are no relationships to other CAs. (Housley, R & Polk, T. 2001. 54)

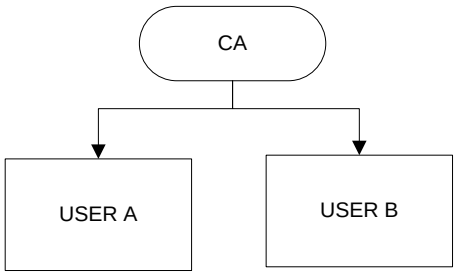


Figure 2 Simple architectures

The Enterprise architecture is more complex. There is one trusted root CA but there can several subordinate CAs. All users trust the same central root CA. The Enterprise solution certification paths are easy to update because every CA has a specific master CA. In the case the certificate is compromised it is easier to update because the certificate is relaying only on that one CA. But if Root CA is compromised all certification and CA must be revoked. (Housley, R & Polk, T. 2001. 57)

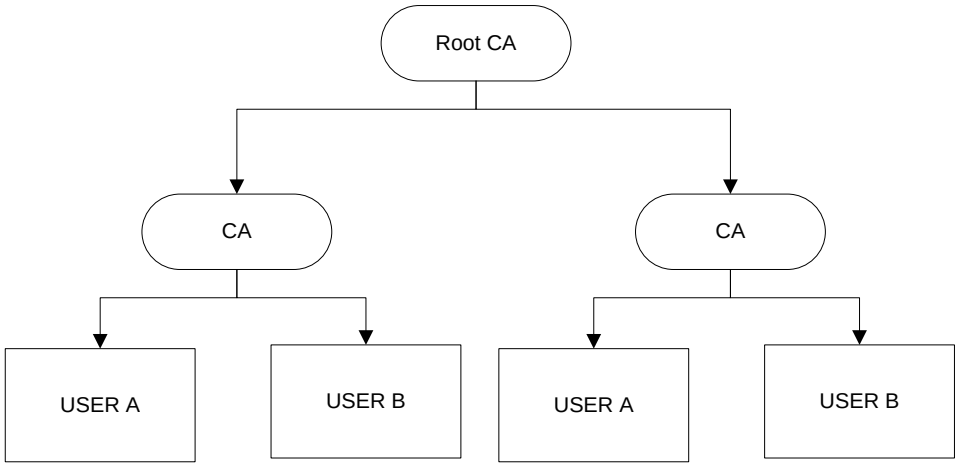


Figure 3 Enterprise architectures

The Hybrid architecture is combination of Simple and Enterprise architectures. A common way is to build peer-to-peer connections between CAs. All Certifications must use same accepted policies and practices. It is more complicated to build a new certification but this guarantees that the secure path is trusted. And this forces CAs to inform right way if CA is compromised. One solution is Bridge CA. In the Bridge solution there is only one CA where parities are trusted. Connection solution is peer-to-peer. All Contacted CAs must follow Bridge CA rules. (Housley, R & Polk, T. 2001. 65)

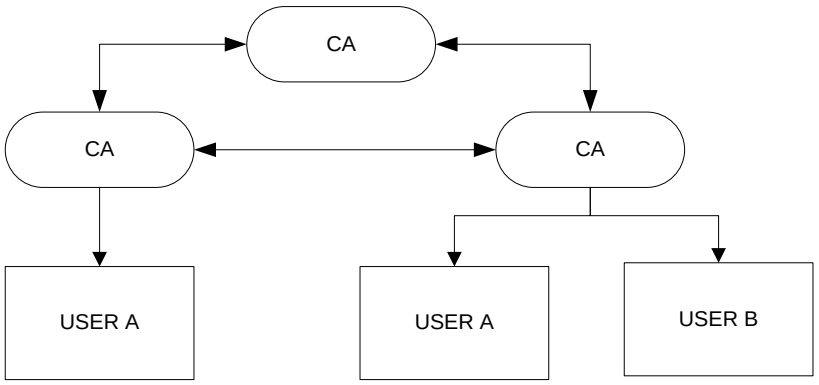


Figure 4 Hybrid architectures

X.509 Certificates has three components. The first component is the tamper-evident envelope. The digital signature provides the tamper—evident wrapper. Inside the envelope there is the basic certificate content. The basic certificate content includes the information that must be present in every certificate. The basic certificate content may include an optional set of certificate extensions. This component contains optional information.

The ideal certificate: (Housley, R & Polk, T. 2001. 21)

- It would be a purely digital object, so it could be distributed over the internet and processed automatically.
- It would contain the name of the user who holds the private key, identify the user's company or organization and include contact information.
- It would be easy to determine if the certificate was issued recently.
- It would be created by a trusted party rather than user who holds the private key.
- Since the trusted party might create a lot of certificates, even for same user, it should be easy to tell them apart.
- It would be easy to determine if the ideal certificate were genuine or forged.
- It would be tamper-proof so on one could change its contents.
- We could immediately determine if the information on our ideal certificate is no longer current.
- We could determine from the certificate the applications to which it applies.

The optional version field describes the syntax of the certificates. The serial number is an integer assigned by the certificate issuer to each certificate. The signature field is an algorithm identifier. The issuer field contains the X.500 distinguished name of the certificate issuer. The validity field has two components, indicating the dates on which the certificate becomes valid and the date on which the certificate expires. (Housley, R & Polk, T. 2001. 74)

Tamper Evident Envelope	Certificate contents		version	v2
			serial number	48
			signature	DSA with SHA-1
			issuer	C=US; O=Hawk; CN=CA1
			validity	010214120000Z to 010214120000Z
			subject	C=US; O=Hawk; OU=R&D; CN=Alice
			subject public key info	RSA, 30 81 89 02 81 81 00 a7 … 01
			issuer unique ID	(usually omitted)
			subject unique ID	(usually omitted)
		Options	extensions	
			signature algorithm	DSA with SHA-1
			signature value	30 2c 02 58 ae 18 7c f2 16 .. 8d 48

Figure 5 X.509 certificate structure
(Housley, R & Polk, T. 2001. 75)

The subject field includes name of the holder of the private key. The subject public key information field contains the subject's public key and algorithm identifier. The issuer unique ID and subject unique ID fields contain identifies and they only appear in versions 2 or 3 certificates. The extension field is used only in version 3 certificates. This field contains one or more extensions. The signature algorithm filed contains an algorithm identifier and it identifies the digital signature algorithm used by the certificate issuer to sing the certificate. The signature value field contains the digital signature. (Housley, R & Polk, T. 2001. 78)

The PKI is used in applications like S/MIME (Secure/Multipurpose Internet Mail Extensions), TLS (transport Protocol Security) and IPsec (Internet Protocol Security). S/MIME version three offer protection for electronic mail. Certification can be used for digital sings and encryption. User can recognize the sender and the mail message is secure. TLS offer authentication and encryption for a communication stream. If both ends are forced to use LTS streams messages are protected. IPsec offers also authentication and encryption for individual datagram. Ipsec uses network layer three. This is a normally used firewall in an outside connection. (Housley, R & Polk, T. 2001. 199)

Key management lifecycle can be divided to four different stages. Each stage has its own functions. With functions management know the stage status about the functions. First stage is Pre-operational stage. Key material is not ready but some keys might be in pre-activation

stage. This stage system and enterprise is being built. Second is the operational stage. This means that keys are in normal use and active. Third is the post-operational stage. Keys are not in active use anymore. Company still has access to the key environment and some case keys can be used. Keys are compromised state. Last stage is destroyed. Keys are not active anymore and not usable. All information about the keys is deleted. Figure 6 Key management states and phases. (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2007. 89)

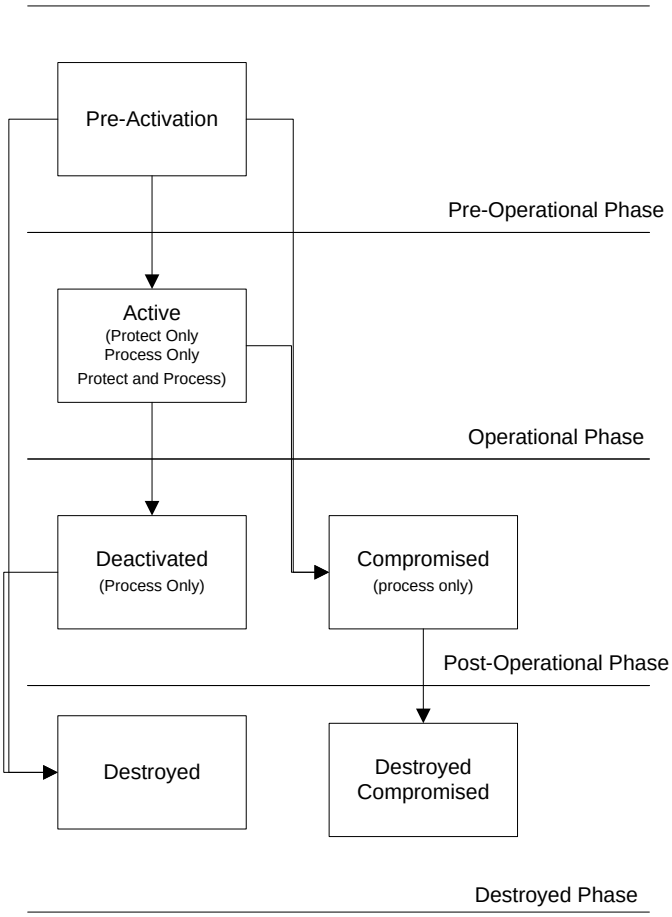


Figure 6 Key management states and phases.
(Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2007. 91)

3 Method

Hevner and Chatterjee write (2010, 5) that design science research is a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts. Results contribute new knowledge. Hevner (2010, 5) also mentions that designed artifacts are useful and basic in understanding environment. The fundamental principle of design science research is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact. “Information systems are implemented within an organization for the purpose of improving the effectiveness and efficiency of that organization.” (Hevner, A., March, S., Park, J. & Ram, S. 2004. 76) Design science

results offer common design knowledge although the professional problem is always unique and prescribed (Järvinen, P. & Järvinen A. 2004. 104). "Research producing field-tested and grounded technological rules differs in several respects from description-driven research" (Van Aken, J. 2004. 231)

In this study the artifact is the Public Key Infrastructure operations model. Design science has two activities: build and evaluate. Artifact is built because that demonstrates how it works. Building is a process of constructing an artifact for a specific purpose like Public Key Infrastructure operations model. Evaluation is the process of determining how well the artifact works and specific criteria must be set up for meaningful evaluation. This also means that when building an artifact like the PKI its operations might be misunderstood. Without understanding the environment the result can be poorly designed in relation to the artifact or the artifact result could have side-effects. When building the artifact these factors must be taken in to consider. (March, S. and Smith, F. 1995.258)

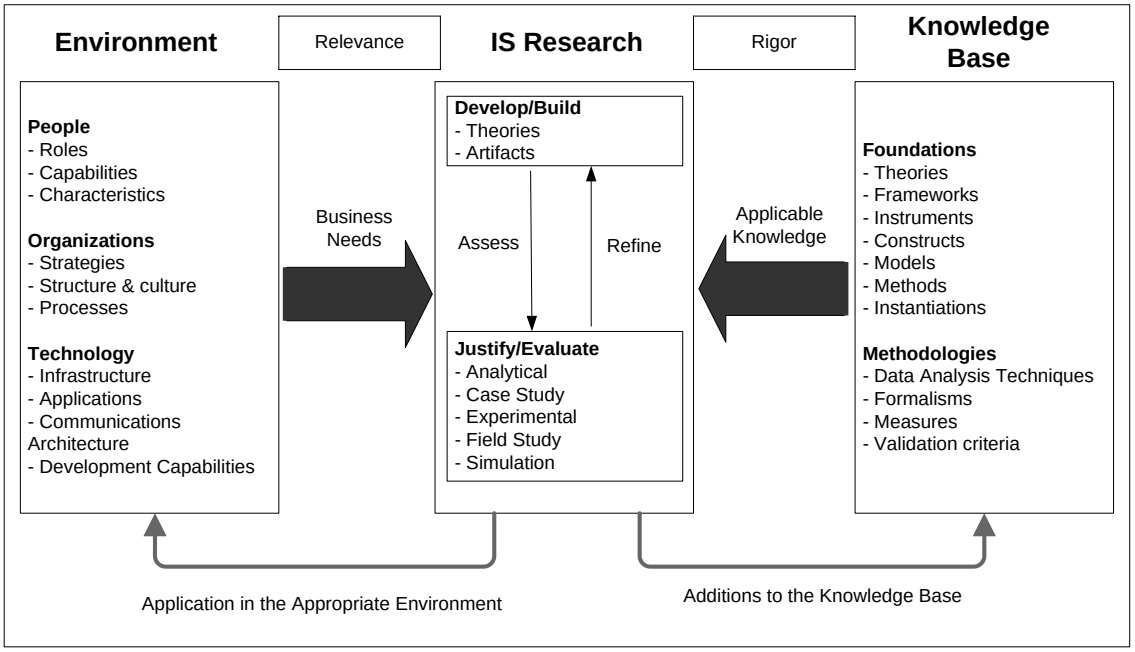


Figure 7 Information Systems Research Framework
(Hevner, A., March, S., Park, J. & Ram, S. 2004. 80)

System development is divided into two main complementary parts: design and behavioral science. Knowledge base is in the design science and the environment is in the behavioral science. Design science paradigm helps develop the artifact so that it can be tested with the behavioral science paradigm. The research goal of behavioral sciences is the truth and in design science research aims for utility. This system development knowledge base provides material to business needs in research. The artifacts are specialized constructs, models, methods, and instantiations. The knowledge base is the foundation of methodologies like foundational theories, frameworks, instruments, constructs, models, methods and instantiations.

Methodologies are guidelines for evaluating results. “Design science research results are codified in the knowledge base, they become best practice.” (Hevner, A., March, S., Park, J. & Ram, S. 2004. 81.)

Hevner defines seven guidelines for understanding information systems research and a clear set of rules or principles proscribed for conducting and evaluating good design science research. (Hevner, A., March, S., Park, J. & Ram, S. 2004. 83)

Design as an Artifact	Design science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation
Problem relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems
Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods
Research contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies
Research rigor	Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact
Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment
Communication of research	Design science research must be presented effectively to both technology-oriented and management-oriented audiences

Figure 8 Design-Science Research Guidelines
(Hevner, A., March, S., Park, J. & Ram, S. 2004. 83)

This thesis use Design science research guidelines to produce research results. Thesis research develops an artifact that is the Public Key Infrastructure operations model. Problem description is how to develop more time, money and a secure way Public Key Infrastructure services. This work is evaluated in real Public Key Infrastructure project. Comparing Public Key Infrastructure model and project research offers result of what is working and what must be de-

velop in future research projects. This thesis should give new information on how Public Key Infrastructure service ought to be built. This paper uses Public Key Infrastructure and security standards and best practices for comparing results. Thesis takes the company project point of view to the results. The results are reported in this public work where all specialists can evaluate them.

4 Public Key Infrastructure operations model

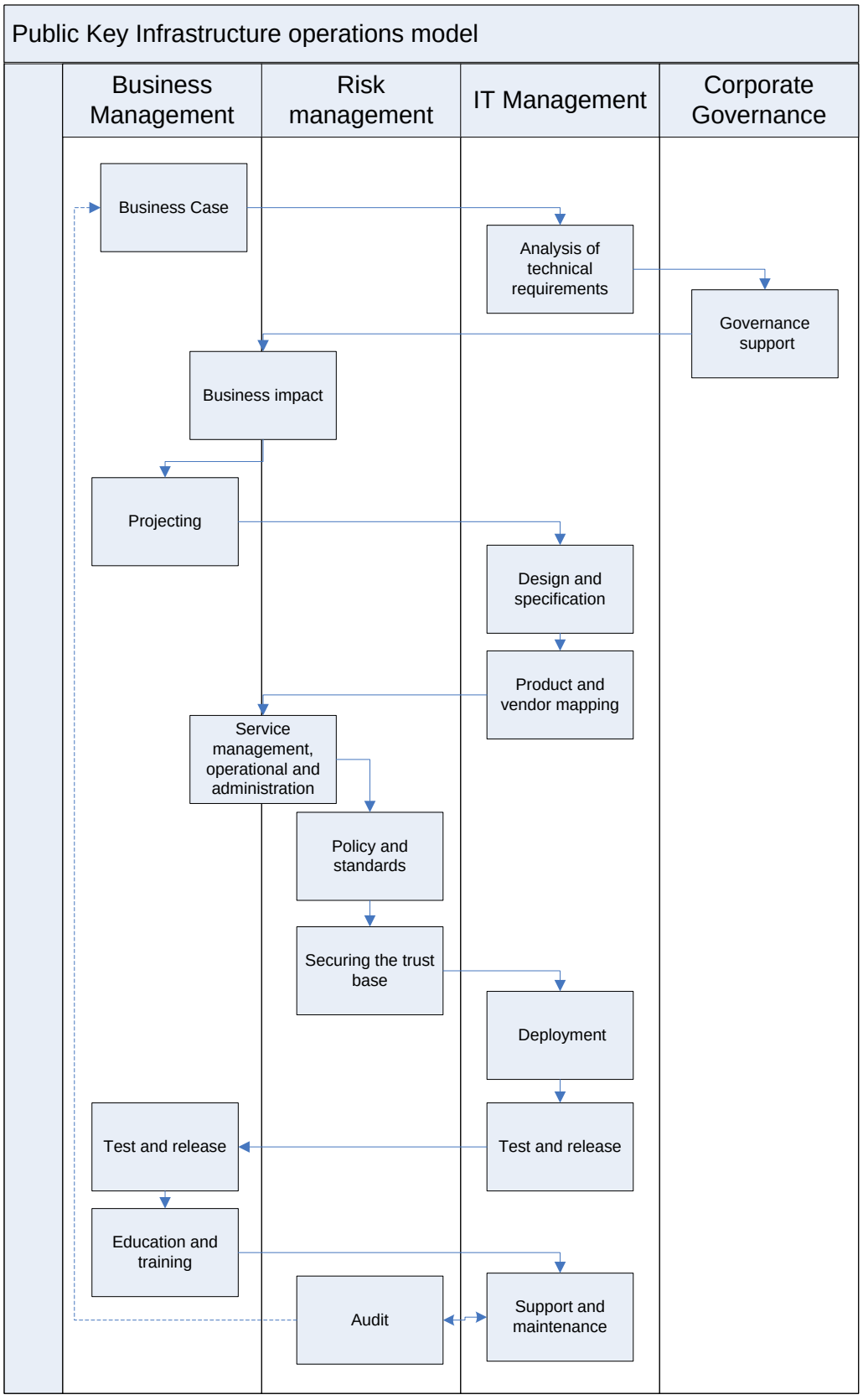


Figure 9 Public Key Infrastructure operations model

Public Key Infrastructure operations model idea is based on ISF (Information Security Forum) best practices and modified for a financial company. The model idea is that it serves as a basic package to new PKI projects. The model is divided to 16 different processes. All these processes have their own role and owners. Process owners have divided to four different roles. Sometimes process significance might be trivial, other times the process might prove vital for the project. Good example is the Policy and standard process. First time a company must build this document, it might be a large undertaking for company. However, in next project this process is only applied for updating valid policies.

Everything starts from a business case. It is important that the business part is leading this conversation. IT management and Risk management is supporting this report. This is an important phase because it is here that most of the metrics are defined. In the end these metrics define how successful the project was. Model is PKI project best practices. This is the reason why all processes are described separate processes. All phases give advice on what must be done and what should be done. In the end it's always a company or project decision what to do in the different kind of PKI projects. This is not a model for how to run a PKI project. It does not concern with how to come up with a project budget, or how to keep project meetings. When a certain project adapts this model it assumes that all basic project process practices are defined beforehand. Normally companies have their own project model what they follow or they can follow PMBOK defined model appendix 1.

4.1 Business Case

Companies should search different options for solution in the analysis phase. All options should have their own cost estimate. Cost estimate must be built up for the current environment situation in the Cost estimate phase and it must have the same elements and be based on identical assumptions. Company should identify each solution benefit in the benefit phase. Result of research must be quantitative if it's possible. Project risks must be identified in the project risk analysis phase. This phase has eight risk categories: Organizational and change management risk, business risk, information risk, technology risk, strategic risk, security risk, privacy risk, and project resources risk. These risks might include cost overruns, schedule problems, vendor problems and privacy details. All risks must be evaluated and the company must have practical solutions for each risk so it has risk-adjusted costs for each solution. Last phase is to evaluate solutions and rank each on cost, benefit and risk order. (National Institute of Standards and Technology 800-35. 2003. 4-9)

The Business case phase must consider what kind of business problems new PKI solution causes. All business processes must be evaluated. Evaluate effects for processes. Cost framework must be designed. There is the implementation cost and operation cost. Company must consider also goals. What new PKI solution gives now and in the future? Also it must consider

benefits like new market, supporting old functions, reduce cost, and increase sales. Company must set detailed plan if the new PKI solution does not work like it was planned. Also it must do a detail impact analysis on existing technical and business environments. The customer or user perspective must be solved also. Company must consider new education and awareness program. Also, all needed PKI skills must be listed so all education costs are visible.

New PKI project might have open issues in requirements. PKI solution is used for the new technology so it is important to use defined standards. Normally some integration and development is needed. This must be taken into consideration because normally this means work load to company's own resources. Business case must consider up level situation CA and RA are compromised. Company must research similar cases from public databases for the best practices. These might give better picture for upcoming projects than own estimates. It is important for the projects that stakeholder expectations are defined. So results are easier to review. Business case must research all legal issues. Also there might be some outside authorities for the different branches' own regulators to follow.

Company should consider a pilot project. It should be done in large scale so all company areas have the possibility to give comments. Pilot project must be light for company. Pilot lowers risks and gives better cost estimate. Also this exposes all fundamental issues like certification usability. This also gives better suggestions how to handle PKI environment in different ways.

4.2 Analysis of technical requirements

Company must investigate to technical requirements. Investigate phase company can use best practices how to validate environments. These give good guidelines what areas company must consider. First is ISO (International Organization for Standardization) 27000 series of standards. ISO 27001 controls are usable. Second is PCI DSS version 1.2 requirements. At least company must consider these details:

- Environment location
- Hardware combination
- Other hardware services
- Disaster recovery
- Hardware security
- Hardware scalability
- Hardware operating system
- PKI software (open or licensed software)
- Hardware limitation (example web service window)
- Web client software
- Auditing possibility

- Known weaknesses

Company must build own key management planning document. This document describes the management of all key management products and services used by a PKI product. This document is valid for the entire PKI lifecycle. One part of this document is the key management infrastructure. The purpose of this document is to ensure that key management services are supportable, available and secure. Specification must follow the organization's resources and technical environment. Especially organization physical protection facilities, security clearances for support personnel and procedures managing cryptographic material must be regulated. The planning process must define critical resources. (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2002. 44)

Key management planning must be tailored according to scope. There are differences between limited email security and full scale network securing projects. This work must be cost effective. The projects must always research all security steps. Good example for this kind of security checklist is NIST (National Institute of Standards and Technology) Special Publication 800-57 checklist (Appendix 2). Some basic steps must be documented always. The key management product and service requirements must be described. These are types, quantities, lifetime and algorithms. Also additional information must be defined. Examples X.509 certificate standard class must be determined. NIST have steps how to define what company need from environment:
(Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2002. 44)

- The types of key management products and services
- List of key management products and services requirements
- The projected quantity of devices to be employed in the application
- The keying material formats
- Lifecycle
- PKI certificate classes
- Tokens or software modules
- Time table when certification are needed
- Project timetable when resources are needed
- Responsible person

Company must understand what requirement PKI needs. This work must be done before any technical decisions. Most important is that business need and model is ready. For example, for the environment effective factor is what kind of purpose certificates are planning to use. One such factor is whether a certification is to be used only internally or will it be applied externally as Important is also the number of certificates now and in the future. Active envi-

ronments must be evaluated also. There might be some similarities so the company may save in expenses.

4.3 Governance support

COBIT define Enterprise governance “It is a set of responsibilities and practices exercised by the board and executive management.”(COBIT Foundation 4.1. 2010. 28) COBIT also define IT governance “it is part of enterprise governance. It is defined as a structure of relationships and processes to direct and control the enterprise toward achieving its goals by adding value while balancing risk versus return over IT and its processes.”(COBIT Foundation 4.1. 2010. 29) Good communication with the wider organization is required to maintain support for the project. This is especially important when dealing with the inevitable difficulties that face any significant systems integration project.

Governance is about performance and conformance. Performance is improving profitability, efficiency, effectiveness, and growth. Conformance is adhering to legislation, internal policies and contractual requirements. (COBIT Foundation 4.1. 2010. 30) Senior management support is needed, specifically a senior manager who supports the project and is prepared to support it through any difficulties encountered during its lifetime. Having good senior management support also helps to open up essential channels of communication across the organization.

Senior managers should be made fully aware of the potential risks in PKI projects and user groups should be informed of what PKI will deliver, how it will work, and what benefits they can expect. One way is to compose enlisting very visible high-level support for the project Also project must create steering committee consisting of persons across the company. Adequate time for public announcements is needed so project stays locked in the minds of the company personnel. Key people for the project must be kept informed of its status. These kinds of functions are RA, CA legal department, personnel, physical security, and support.

4.4 Business impact

Typically business impact cost is divided into four different cost sections, the first being project management and operational and maintenance support costs. Next are hardware and software costs which form the basis of the PKI. Third is training costs, external consultant services and security audits. Last are legal and policy requirements. Company must consider how key areas are impacted. With new environment there might become new channels to market or some process can be automated because of better security. There might be some changes to desktops or mobile equipment. Also some network might come. Certificate handling might change. There might become new certification processes. This affects also CRL

and policy performance. Last are end user changes. For example, this might affect remote access connection processes or authentication methods like single sing on.

All actors, including business partners, customers and other vendors, must be informed of these changes. These actors must be fully briefed and provided documentation about the changes and how the changes affect them. Also own education and awareness events and senior management consultation should be arranged. They management and company personnel also need detailed information on what has changed. In security changes there is always a risk on one's reputation. Backup plans are essential for survival if public reputation is at risk.

4.5 Projecting

In the projecting phase the first thing is to check if a company has its own project model to follow. Company members must confirm that technical content, quality, time, and costs are managed. Normally an outsider consult or a specialist is needed. Typically they utilize their own models that they are used to applying. Below is one example on how to proceed:

- Requirements analysis for business drivers, analysis of costs, business benefits, alternative solutions, system vulnerabilities, security requirements, legal and regulatory constraints, project planning
- Definition for designing and modeling the proposed PKI architecture, trust management, defining operating requirements, specifying test activities, producing the detailed project plan
- Operations for definition of the operating procedures and controls, production of the Certificate Policy and Certification Practice Statement
- Security review, corrective action
- Integration for system build and test, operator and support training
- Deployment for installation and validation, acceptance testing
- Post-deployment for upgrading, operation testing.

PKI projects are complex undertakings that often involve a large number of vendors and service providers. These must be carefully controlled in what activities they are taking. For example, configuration management must have a clear picture of version control of all operating system software and PKI component software. Also, Change management must make sure that all implication to PKI design is understood. Outside consults and specialists normally cost a sizable sum.

Here are some risks that must be controlled in the PKI project:

- Interoperability with the corporate directory

- Identifying and retaining skilled resources
- Integration with applications
- Impact upon the existing IT infrastructure
- Interoperability with other PKI elements like CA and RA
- Scalability and performance.

4.6 Design and specification

A wide variety of factors affect the design of a PKI. Design must be such as to ensure that it is capable of meeting the organization's instant and future requirements. European payment council recommends that "Asymmetric key pair should be dedicated to one usage for instance: entity authentication, non-repudiation of data, symmetric keys encryption or other" (European Payments Council.2009. 67). All security needs and certificate requirements for company must be researched following before before and after the company makes any decisions: (Microsoft Window Server TechNet Library. 2003.)

- Location of the root certification authorities.
- Internal versus third-party CAs.
- Requirements for CA capacity, performance, and scalability.
- User management structure.
- Your PKI management model.
- CA types and roles.
- Use of hardware cryptographic service providers.
- Number of CAs required.

CA infrastructures consist of a hierarchy of CAs. The infrastructure's final authority is called root CA. The root CA certifies other certification authorities to publish and manage certificates within the organization. After these definitions, the project can define roles for any additional certification authorities, including who manages them and what trust relationships they have with other CAs. These must be defined for specifications: (Microsoft Window Server TechNet Library. 2003.)

- Person or team who designates the root CA in the organization.
- Where the root CA is to be located.
- Person or team who manages the root CA.
- Is the root CA role only to certify other certification authorities or also to serve certificate requests from users.

Organizations must define CA capacity, performance and scalability. Companies must know how many certifications they need to issue and renew. They must define the lengths of issuing CA certificates and number of configurations what client computers must support. Hardware and network definitions must be specified also. If the company uses lot of small CAs with strategically located CRL distribution points, it reduces the risk that your organization might be forced to revoke and reissue all its certificates. This case is current if a large CA is compromised. If company uses lot of CAs this might increase administrative overhead. (Microsoft Window Server TechNet Library. 2003.)

Companies must also outline network capacity so roles are clear. Network is more vital than physical performance limitations. When company is planning server and network environment specifications to PKI the company must consider number of CPUs (Central Processing Unit), disk performance, number of disks, amount of memory, and hard disk capacity. When companies define environment they must take into consideration key length and network bandwidth. Companies must define PKI group policy. This includes trusted root for groups of computers, certificate trust list and auto enrollment. (Microsoft Window Server TechNet Library. 2003.)

It is vital to define a PKI management model before company starts process design CA infrastructure. PKI management model must complement company security management design and it gives requirements for roles (appendix 3). Company must remember at specifications that single individual cannot compromise PKI services (appendix 3). It is always better to spread roles across company. The following tasks must be spread: (Microsoft Window Server TechNet Library. 2003.)

- Creating or modifying CAs
- Managing certificate templates
- Issuing cross certificates
- Issuing or revoking user certificates
- Configuring and viewing audit logs

Company must define CA types and roles. Microsoft Windows Server uses two services. These are enterprise and Stand-alone. The difference between these two is that enterprise is integrated into Windows own Active Directory. Company must design also Root CA and Subordinate CAs. Microsoft has built guidelines to design CA (appendix 4). Company must also choose CA architecture from three alternatives: simple, enterprise or hybrid. It must also define different CA roles in the architecture. These can be divided, for example, to security classes: basic, medium or high. Also firm must define CA naming standard. At this stage company must have a plan on whether they need to use third party CA for cross certification requirements.

At this stage the company must specificity its CA environment disaster recovery and continuity plans. CRL behavior must be determined. Is CRL list single, multiple or online revocation? (Microsoft Window Server TechNet Library. 2003.)

4.7 Product and vendor mapping

The main question is, are PKI services hosted by the company or outsourced. Vendor selection must be based on offered functions and those criterions. For example, vendor product components supply for different PKI solutions, vendor product flexibility, reputation, financial situation, market status and segment, customer references, location, standards what they use, support, consulting and development capability, and understanding of the operating environment.

The next task for the company is to select product. Mainly this means that company must compare their requirements to what the product support. These kind of requirements are PKI architecture, product maturity, ability customize, what standards are supported, key and certificate management, security management, hardware, network and operating system requirements, and product support lifecycle.

Firms can also build their own solutions. What this means is that the company must to maintain direct control over its security policies. Also, the company must align its certificate policy with security policy. Their own solution can be expanded to include additional functionality and users at relatively little extra cost. But this means also that company manages its own certificates and manages software and hardware updates. This requires an in-house dedicated staff because project deployment schedule for internal CAs is longer than third-party service. Businesses must likewise accept their responsibility for the PKI environment. Furthermore, the end customer point of view must be kept in mind. Certification liability must be trusted also to the customer. Sometimes cross certification is needed.

Companies can focus on core business for outsourced PKI solutions. The outsource vendor is responsible for technology changes and liable for security. Companies can build their trust toward their outsource vendor using PKI standards. They do not need hire any specialist to host PKI environment. Typically, costs are shared per certificate so costs might turn expensive in a large environment. Quick changes are not possible and environment is not so flexible. New integrations might prove difficult to do. In the end, the individual business is always responsible for security issues to the end customer. Contracts are vital to outsourcing PKI services. ITIL (Information Technology Infrastructure Library) has listed what must be taken into consideration when outsourcing: (Cazemier, J., Overbeek, P. & Peters, L. 2010. 115)

- Protect company assets, including information, software and hardware
- Determine any compromise of assets
- Controls to ensure return or destruction of information and assets
- Reporting structure
- Change management process
- Authorization processes
- Arrangements for security incidents and breaches
- Audit processes
- Service continuity requirements
- Third party subcontractor agreements
- Termination or agreements

4.8 Service management, operational and administration

In ITIL, the four main functions are service desk, technical management, IT operations management, and Application management. Technical management, IT operations management and Application management contain number of operational activities to ensure service and processes. These ensure technology required by delivers and support service is operating effectively. (Cazemier, J., Overbeek, P. & Peters, L. 2010. 88)

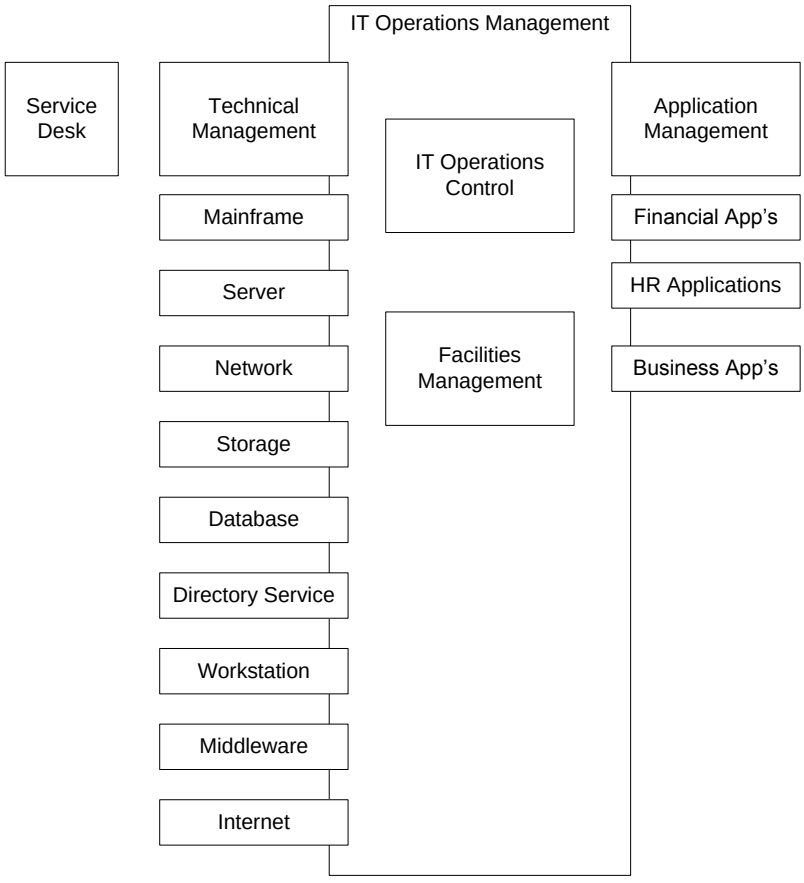


Figure 10 Service operations functions
(Cazemier, J. 2010. 88)

Information security management has responsibility for setting policies, standards and procedures to ensure the protection of the company assets, data, information and IT services. Operational management cannot own security management function. Operational service team executes security policies, standards and procedures. It also gives technical assistance and does technical security controls. (Cazemier, J., Overbeek, P. & Peters, L. 2010. 89) Operational requirements are for PKI environment: (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2002. 63)

- Certificate Application
- Certificate Issuance
- Certificate Acceptance
- Certificate Suspension and Revocation
- Security Audit Procedures
- Records Archival
- Key Changeover
- Compromise and Disaster Recovery
- CA Termination

Clear guidelines on the operational procedures must be specified so operational teams can understand what actions they are required to do and what actions are outside their responsibility. Operational team actions are listed in appendix 5. Regular reviews of services must be held between operational and security teams. Annual reviews with the service provider must also be held. For the PKI environment few add-ons should be considered. First is the specification of the service management criteria required for the PKI. Next involves the definition of the operating procedures for the management of the trust services like CA and RA. Last is the definition of liability for outsourced certification or registration.

4.9 Policy and standards

Bank for Internal settlements principle 15 defines policies in the following manner: “Supervisors must be satisfied that banks have in place risk management policies and processes to identify, assess, monitor and control or mitigate operational risk. These policies and processes should be commensurate with the size and complexity of the bank.” (Bank for International Settlements. 2006.4). PCI card industry definition of policies reads that “A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.” (PCI Security Standards Council LLC. 2008.64).

Public key infrastructure Certificate Policy (CP) framework rfc3647 is published by Internet Engineering Task Force (See Appendix 6). Certificate policy must inform the reader of what you have. Certification Practice Statement (CPS) must tell the reader how to use Certificate Policy guidelines. Certification Policy is divided nine main points. It is necessary to go through each of these main points so that all the subjects of the Certificate Policy are covered. Certificate Policy functions as a part in the company's overall security policy. Also some Certificate Policy issues might be found in other company policies or agreements. Certificate Policy must be readable for the readers so they understand what they are reading.

Certificate Policy consists of directions from management. One involves creating a key management program, next is about establishing its goals, and the third deals with assigning responsibilities. Security Policy submits matters such as the specific managerial decisions. These establish key management infrastructures and the generation, distribution, securing, and accounting for keying materials. (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2002.65). This is reason why Security Policy must define the roles, responsibilities and key management activities.

Standard is a larger subject to focus on Public Key Infrastructure operations model. Standards are more top-level tools for handling Public Key Infrastructure issues. Still, there are always good guidelines for to follow. The best known security standard is the International Standardization Organization (ISO) 27000 series. It describes the management system of information security. There is no direct connection to PKI but lot of usable guidelines. Other usable ISO standards are 13335:2004 management of information and communication technology security, ISO 7498-2 OSI Security Architecture and ISO 20000 Service Management. There are also models and associations which provide guidelines. One Is the International Security Forum's (ISF) standard of good practice for information security, while another is the Sherwood Business Security Architecture (SABSA). The latter model focuses on architecture security, taking into consideration all critical functions. There are also the Information System Audit and Control Association (ISACA) COBIT model, Security Standards Council PCI model, and National Institute of Standards and Technology Special Publications.

4.10 Securing the trust base

Securing the trust base is the base of on Certificate policy. PKI requirement is to ensure that Certificate Authority, Registration Authority and certificate repository are properly protected. First is physical security. Company must make sure that Certification Authority and certificate repository are housed in a physically secure location. Access to Registration Authorities and Certification Authorities should be controlled by using two factor authentications.

Next is the network security. Services are locating the Certification Authority and certificate repository behind a dedicated firewall. This should be configured to pass only LDAP (Lightweight Directory Access Protocol) traffic to the repository and certificate management traffic to the Certification Authority. PCI model defines network security “Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.” (PCI Security Standards Council LLC. 2008.55).

Third in the list is the computer security of the operating system on those machines on which the Certification Authority and repository will run. Vulnerability assessment tools must be used other ways to support this activity. The PCI rule defines operating system danger as “Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches.” (PCI Security Standards Council LLC. 2008.38).

Fourth is intrusion detection. Implement intrusion detection software on the LAN segment housing the Certification Authority and certificate repository. Host-based intrusion detection software should be placed on the Certification Authority and certificate repository server machines. Penetration testing should be conducted on a regular basis and whenever there has been any significant change in the computing base.

Fifth is Availability. The certificate repository should be designed for high-availability.

Last is the operational security. Certification Authority administrators should have the highest level of security clearance in the company. All relevant logs and alerts should be reviewed on a daily basis.

The company must make sure that Security education and awareness activities are carried out. PKI users also need to be periodically reminded of the need to protect their private keys. Disaster recovery plans must be developed and maintained that detail the steps to be taken should a catastrophic event occur. These should specify the precise actions to be taken to recover the PKI at an alternative secure location. Particular attention will need to be paid to maintaining the level of security that is required to ensure the proper protection of the Certification Authority. Clear procedures for dealing with compromise or suspected compromise

need to be developed, implemented and communicated widely to PKI users, support personnel, and help desk staff.

Company must maintain and analyze audit logs for unusual or suspicious events. All significant events in the trust base should be recorded in a secure audit log with key events time/date stamped and signed to prevent unauthorized changes. Also ensure that the trusted computing base is maintained and that any changes are detected, investigated and corrected. Company must ensure physical security controls are strictly maintained and that only a limited number of known trusted administrators have access to the trust base machines. Company must set rules to all visiting personnel ensuring they are escorted at all times and that all actions are underwritten, clearly understood and checked.

Incident response guidelines what company should do minimum:

- Immediate action
- Impact analysis
- Root cause analysis
- Escalation to senior management
- Communication to staff, senior management and press office

4.11 Deployment

The company must have detailed plan on how to deploy the PKI. Here the first step is the schedule rollout. It's possible to do partial rollout and publish rest of the services, such as secure mail function or smart card authentication, later when the business needs these. Next phase is the installation of Certification Authorizes. Company must have its CA hierarchy ready. After this hierarchy stage and offline root CA must be installed. After this the following stage is the publishing of the offline CA certificate and application of CA policy. The Authority Information Access (AIA) and CRL distribution point (CDP) extensions follow after this part. The AIA extension specifies where to find the latest certificates for the CA, while the CDP extension stipulates where are the newest CRLs. These extensions are issued by that CA and ensure that this information is included in every certificate that the CA issues so the certificate is available to all clients. (Microsoft Window Server TechNet Library. 2003.)

Configuring certificate templates is the next stage. After that Access Control Lists (ACLs) for each certificate template control the permissions is needed to request certificate types. Next phase is to configure public key group policy and configure CRL Publication. After this the company must decide what the default certificate publication period is and ensure application reliability because many systems rely on CRL availability. CRL size and cleaning procedures must be on production. One of the central things in the deployment phase is to dele-

gate CA Administrators so they understand their responsibilities. After this the company can configure certificate enrollment and renewal processes and start issuing certificates. (Microsoft Window Server TechNet Library. 2003.)

For large deployments a slow, staged rollout in which each stage can be reversed, if necessary, is recommended. The deployment of a PKI can be one of the most time consuming and expensive parts of the entire project. Where PKI client software forms part of the solution it will be necessary to visit every desktop, laptop and other computing device that needs to make use of the PKI. The user base and education and awareness activities must be completed prior to installing the client software. Where the roll-out actively introduces the user immediately into the PKI, following material should be provided to ensure that users fully understand the importance of protecting access to their keys and they are aware of how the PKI affects their job. Also realize the limitations of the PKI and know where and how to get help.

There are six development functions: (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2007. 92)

- User registration function
- System initialization function
- User initialization function
- Keying material installation function
- Key establishment function
- Key registration function

Pre operational phase in user registration function is crucial so that the RA establish appropriate procedures for the validation of identity. This might be face to face identification or some other strong authentication method. The strength or weakness of a security infrastructure depend the identification process. System initialization function is to build or configure a system for secure operation. User initialization function is about installation of a key at a CA, trust parameters, policies, trusted parties, and algorithm preferences. Keying material installation function is how to set up hardware, system, application, crypto module or devices. Key establishment function is the generation and distribution. Key registration function is the binding of keying material to information or attributes associated with a particular entity. (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2007. 92)

4.12 Test and release

PCI definition for the testing reads: “Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System compo-

nents, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment." (PCI Security Standards Council LLC. 2008.59). Tests must be done in a proper way if the Public Key Infrastructure is to be secure and functional. Company should form the quality control points that determine if the project can proceed or not. Test data is used to determine to check that the system is working correctly. This is important in the case of keying material. The Certification Authority signing key should also be securely disposed of to ensure all certificates that were signed by it during testing are no longer valid. Also, this should assess to what extent the implemented PKI meets the documented design requirements. The project must at least test the Certification Authority installations, Registration Authority installations, PKI client software installations and performance.

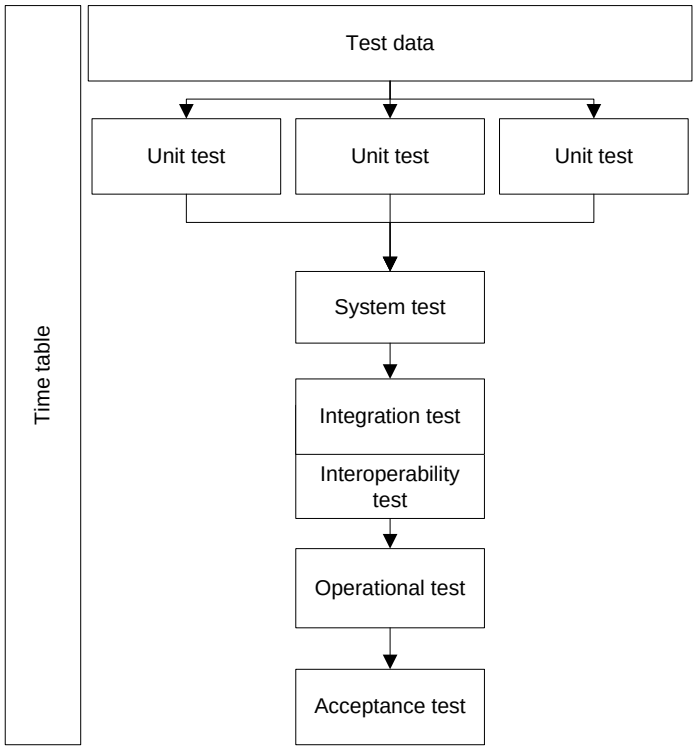


Figure 11 Test process

The project must construct a reliable test schedule before actual testing starts. After this the project must generate test data and then the unit testing can begin. After unit tests system tests are the next step. Integration tests start when connections to other end points are ready. These tests include also interoperability tests. These tests exam CA usability to other CAs. After this an operational test must be done in an environment which looks like the production environment. Last is the acceptance test. This is a test area where the project needs business effort to finalize the version for production.

National Institute of Standards and Technology Special has defined testing for the CKMS (Cryptographic Key Management Systems):(Barker,E., Branstad,D., Chokhani,S. & Smid,M. 2010.63)

- Vender Testing
- Third Party Testing
- Interoperability Testing
- Self-Testing
- Scalability Testing
- Functional Testing and Security Testing
- Limitations of Testing

4.13 Education and training

All users must share a clear view of the protection measures they must provide for their private signing key. Furthermore, they must always be aware of what they are signing and fully understand the purpose and function of the PKI. An example for this is how the new PKI environment changes personnel work. With the new environment come new responsibilities for the personnel. Normal security issues must be found from Security Practice Statement document.

PKI operating personnel education points:

- the security operating requirements of the PKI
- the function and purpose of the PKI
- how to operate the PKI
- how to resolve day-to-day issues
- how to recognize potential security issues and escalate them.

	AWARENESS	**TRAINING**	**EDUCATION**
Attribute:	What	How	Why
Level:	Information	Knowledge	Insight
Teaching Method:	Recognition	Skill	Understanding
Test Measure:	Media - Videos - Newsletters - Posters	Practical Instruction - Lecture Case study workshops -Hands-on practice	Theoretical Instruction - Discussion Seminar - Mackground reading
Impact Timeframe:	Short-term	Intermediate	Long-term

Figure 12 Comparative Framework
(NIST 800-12. 1995. 147)

NIST has three separate terms: awareness, training, and education. Awareness supports the mission of the company by valuable recourses. From a personnel's point of view it is merely some rules and procedures. In a normal case they ignore those and do not make any suggestions for improving security or recognizing any threats. Training is about teaching the personnel such skills that they can perform their works tasks in a more secure way. This means that ideally they should know what to do and how to do it in a secure way. Training is divided into basic security tasks and more technical security issues. It is effective when tailored to specific audiences as then the contents can be more detailed and specific. Tellingly, the education designed for security professionals often focuses on the particulars of just one or two issues. (NIST 800-12. 1995. 147)

Awareness, training, and education boil down to the all-important question of communication. All three activities are focused on understanding what the interests of the information security management mean and to guide personnel and customer toward these interests. Normally, changing old processes is difficult for the company personnel who do not like having their privileges removed, even when they are not really needed. The personnel need to be convinced why the changes are made. This new PKI Awareness, training and education program must add company's normal instructions for the new personnel or new position. (Cazemier, J., Overbeek, P. & Peters, L. 2010. 94)

4.14 Support and maintenance

NIST definitions for support and maintenance form the last three stages of the key management lifecycle. These are operational stage, post-operational stage, and destroyed stage. Operational stage is divided into four sub phases. First is the normal operational storage function with device or module storage and immediately accessible storage. Second is the continuity of operations function. This includes backup storage and key recovery functions. Third is the key change function what includes functions re-keying and key updating. Last is the key derivation function. (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2007. 102)

ITIL definition to service operations processes are: (Cazemier, J., Overbeek, P. & Peters, L. 2010. 77)

- Event management
- Request fulfillment
- Incident management
- Problem management
- Access management

Event management is a detectable or discernible occurrence that has an impact to service. Deviation might cause a service break. It is important that the business is informed when security events occur. Request fulfillment is a process that deals with service requests. It is controlled by the PKI or other policy documents. Incident management is how the company uses continuity. These cases are divided into five sub areas: legal issues, broad incident analysis, estimating damage, restricting unnecessary damage, and restricting the knowledge of security incident. (Cazemier, J., Overbeek, P. & Peters, L. 2010. 78)

Problem management aims to find causes to incidents, making it possible to find security leaks. Few points must be remembered. First is to keep problem management team on a need to know basis. This means that it is better that the team is too small than too large. Also, when new findings are located it is important that security solutions do not cause further security problems. Access management is about the authorization of the environment and documentation. (Cazemier, J., Overbeek, P. & Peters, L. 2010. 85)

Hardware and software must be monitored to ensure it continues to meet the performance and reliability requirements of the PKI. Software patches and bug fixes are needed to be evaluated beforehand and then installed in a controlled way. Helpdesk for PKI users must be single point of contact. Call management procedures must forward the issue to the second and third line support functions. This way company can ensure that problems are addressed as soon as possible. Helpdesk staff must be trained to recognize scale of security problems so they can forward the information to the function responsible. A single 24 x 7 contact point for all security-related queries should be established so that PKI users so users can report any suspicious activity or key compromise without delay.

4.15 Audit

Bank of International Settlements definition for audit is “Supervisors must be satisfied that banks have in place internal controls that are adequate for the size and complexity of their business. These should include clear arrangements for delegating authority and responsibility” (Bank for International Settlements. 2006.4). Part of the audit management process company must define the roles and responsibilities of the users who are involved in the management. List of possible users: (European Payments Council. 2010. 9)

- Business users
- Help desk / customer support
- Systems management users
- Contract management
- Internal & external auditors
- Security administrators

- Internal investigation teams
- Computer Security incident response team
- Law enforcement agencies

Two types of audit must be performed. First is to audit security plans and procedures. These must be on the same level as the certification policy. Second audit form is the technical approach. All critical technical solutions must be audited. These inspections must also be comparable to the policies. Both of these audits must be performed periodically as it is specified in the certification policy. (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2007. 114).

The company in question must make sure at the audit that proper administration and applicable infrastructure controls exist for implementation, maintenance, and usage of private key encryption. Also, key management, including generation, maintenance, distribution and expiration, is to be controlled. Company must have evaluation of private key alternative methods take into consideration the company position on need for security. The Information Systems Audit and Control Association and Foundation published audit steps appendix 7 and questionnaire to PKI environment audit appendix 8. (The Information Systems Audit and Control Association and Foundation. 2001.3)

5 Findings

Business case phase is a regular business case process. This process should come from company's own process environment. There are no specific PKI demands in the business case phase. From a security point of view these phases should have their own detailed guide on how to estimate what are the costs to security environment. How to estimate what is really needed so future projects do not build extra secure or fully automated environments without any benefit.

In the analysis of technical requirements the company should follow know standards like ISO 27000 or PCI. Good example is best practices like appendix 2. It is important to go through all in the analysis stage as the company can easily notice if some area, like the physical environment, is missing. Normally projects think only for valid environments. There might be similarities and projects can save cost and time. Also, if environment is outsources it helps environment deployment.

Governance support like senior management support is vital for the security projects. These are persons who can make decisions so projects avoid delays because of lack of decisions. Model gives basic knowledge for governance support but this is normally depended on compa-

ny or project manager. For example, inside project manager has better connections to senior management. Sometimes this is a good thing and at other times this is a problem.

Business impact phase needs more detail information how to evaluate real impact. For example this phase needs a check list for the actors like customer, personnel, and vendors. There is always something what must be taken in the consideration. That is the reason why best practice check list is needed. This phase is also related on company sector. Different sectors have own demand and needs.

Projecting phase is a standard stage in the projects. This phase is not so important in this model. This phase should give more detail information where project manager can find guidelines and best practices on how to set up a project. There is good models to follow like the PRINCE2 (Project IN Controlled Environment) or PMBOK. Company should have its own model what to follow. Some PKI project cases are good to follow a vendor or consult specified project model if they are responsible for the project.

Design and specification phase is what to write so an environment can be done. This is more technical than others. It is important that technical personnel of the project are participating. This Microsoft guideline for implementation is enough for the windows environment. I assume that other service providers have same kind of best practices what to follow. At this phase all business needs must be known by the project design group. These specifications should be reviewed with the business.

Product and vendor mapping phase are decisions what service provider or program company are using. This phase needs more information example from ITIL. From ITIL project can find of processes for finding right product and vendor. For example, there should be specified RFO (Request for Order) and RFP (Request for Proposal) processes. This is normally specified in the company because it works with all projects. Service management, operational and administration phase is fully implemented from ITIL. Maybe some special detail for PKI or security can be found. Basically these processes are almost same in all IT sector. Model should follow ITIL process steps with PKI information.

The policy and standards phase is more detailed to PKI and security issues. PKI and security have their own security policies and practice statement models what to follow. During this phase it is always important to remember that companies have their own security policies what they must follow.

Securing the trust base phase tells company what was the PKI policy state because this phase is based on that. In this phase all the PKI policy stages must be checked so that all is done as

in the defined policy. PKI policy is an inclusive guide, ranging from technical to legal issues. So this phase needs time to pass. Deployment phase is about the technical issues. In this phase all plans are built to use. It is very important to follow specifications so all is done in the right order and in the right way. Normally in this phase it is noticed whether something is not planned. These new specification add-ons must be described and approved by the management. Also it is import calculate new costs.

Test and release phase is where project needs more hands on personnel because there are lots of different tasks. Normal situation a company has its own test and release processes. If not company should follow some known standard or best practice like ITIL. ITIL has already solved basic problems with this phase. This implementation model should follow more ITIL process. These basic ITIL processes need all kind of authorities.

Education and training phase is easiest to drop out from the plans. Yet it is still an important part. This phase is for the new users and for the rest of the company to know what this project focuses on. Company should have its own security education and training program. This should be only one part of that. Project has massive work to do if company does not have any program of its own. This must be taken care of in the project time table.

Support and maintenance phase is important for continuity. Company should have already working support and maintenance processes. This is only for PKI implementation to that. Also this is lighter if services are outsourced because of some services are provided by the vendor. Company should follow ITIL processes if company does not have already these processes on place. During this phase the company must consider whether the PKI services are open always or can the hours be limited to business hours.

The audit phase is compulsory for some sectors. This means that company should have an audit process on place like specification audits and environment audits. Normally these are added to company's own project processes. During the audit phase the company should use COBIT models. Company separate full COBIT implementation from project work.

This model phases is not same operational level. Some phases are light business decisions and so are detailed technical assignments. Model needs some kind of estimation about the timetable. Every phase should have its own duration estimate. Also, the model needs an estimate on what phases can be done at the same time and what phases are depended on each other. It also needs actors. Every phase should have information concerning who is responsible for that phase and who must participate in that phase. Project manager carries the overall responsibility but every phase needs its own responsible person such as the audit risk manager or for technical environment setups the technical architect.

6 Conclusions

My thesis has developed a particular artifact: a Public Key Infrastructure operations model. This model offers first steps on what must be done in a Public Key Infrastructure project. It also gives a partial answer on how to develop better PKI services. So time and money is saved and Public Key Infrastructure services are more secure. Results are from a real Public Key Infrastructure project but these kinds of projects are comparable with one another.

Public Key Infrastructure operations model should build be based on some known standard or best practice. Most suitable are the base ITIL with COBIT extensions. This is the case especially when ITIL is used in the other projects. When the base model is ready that can be evaluated by the CMMI (Capability Maturity Model Integration) so company knows what the model performance is. After this, the model should have its own security extensions. Last comes the Public Key Infrastructure extensions to operations model. A model without generalizability is not reusable. Public Key Infrastructure is very usable in various situations. This is one more reason why the base model should be based on some known model.

The PKI product provides technical best practices guides to companies like Microsoft development guide to Windows server 2003. But full usable best practice model is not readily available. There is always some kind of risk in the use of best practice models or standards. David Lacey mentions at his article “We have a dangerous herd mentality setting in, to the point that best practices can now be considered dangerous. Whether it’s methodologies, control descriptions or technologies, we are locked into a dangerous monoculture which is leading to a growing systemic risk.” (Lacey, D. 2011)

7 Further research

Future research could involve comparing Public Key Infrastructure operations model to ITIL models or to some other widely used model. Researchers should build a new base for the Public Key Infrastructure operations model following the comparisons. This model issue is better divided into smaller phases so it is easier to develop. Good example for next step development is an own check list to every phase. Model of this kind research could use PCI standard.

The model must be updated regularly because Public Key Infrastructure is constantly developing. There comes new ways to use the environment or the technique changes. Basically, security is going forward all the time. This means that model updating process is needed. This could be implementation from ITIL or COBIT.

References

Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2007. Recommendation for Key Management – Part 1: General. National Institute of Standards and Technology - Special Publication 800-57.

Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2002. Recommendation for Key Management – Part 2: Best Practices for Key Management Organization. National Institute of Standards and Technology - Special Publication 800-57.

Barker,E., Branstad,D., Chokhani,S. & Smid,M. 2010. A Framework for Designing Cryptographic Key Management Systems. National Institute of Standards and Technology Special Publication 800-130

Cazemier, J., Overbeek, P. & Peters, L. 2012. Information security management with ITIL V3. Van Haren publishing.

Cobit Foundation 4.1. 2010. Student handbook version 1.0. The IT Governance Institute

Federation of Finnish Financial Services. 2011. Tupas Identification Service – Identification Principles, version 2.0b.

Feistel H. 1973. Cryptography and computer privacy. Scientific American – volume 228, number 5.

European Commission. 2010. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the religions. A Digital Agenda for Europe

European Payment Council. 2009. Guidelines on algorithms usage and key management. EPC342-08

European Payments Council. 2010. The use of audit trails in security systems: guidelines for European banks.

A Guide to the Project Management Body of Knowledge (PMBOK guide) Third Edition. 2004. Project management Institute.

Hevner, A & Chatterjee, S. 2010. Design Research in Information Systems - Theory and Practice. Springer New York Dordrecht Heidelberg London

Hevner, A., March, S., Park, J. & Ram, S. 2004. Design science in Information Systems Research. MIS Quarterly (28:1).

Housley, R & Polk, T. Planning for PKI. John Wiley & Sons, Inc. 2001

The Information Systems Audit and Control Association & Foundation. 2001. eCommerce Security Public Key Infrastructure Symmetrical (Private) Key Encryption Audit program and internal control questionnaire.

The IT Governance Institute. 2007. Cobit 4.1.

Järvinen, P. & Järvinen A. 2004. Tutkimustyön metodeista. Tampereen Yliopistopaiono Oy.

Kontkanen, E. 2008. Pankkitoiminnan käsikirja. Finanssi- ja vakuutuskustannnus.

March, S. and Smith, F. 1995. Design and Natural Science Research on Information Technology - Decision Support Systems, vol 15, no 4, pp 251-266.pdf

Mattord, H & Whitman, E. 2010. Management of information security. Third edition. Course Technology.

Ministry of Defence. 2011. Finnish national security authority – National security auditing criteria (KATAKRI) version II (English).

Ministry of the Interior, Finland. Act on Electronic Signatures (14/2003)

Ministry of the Interior, Finland. Act on Preventing and Clearing Money Laundering and Terrorist Financing (503/2008; amendments up to 918/2008 included).

National Institute of Standards and Technology. 2003. Guide to Information Technology Security Services - Special Publication 800-35.

National Institute of Standards and Technology Special Publication 800-12. 1995. An Introduction to Computer Security: The NIST Handbook

PCI Security Standards Council LLC. 2010. Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures. Version 2.0.

Shannon C. E. 1949. Communication Theory of Secrecy Systems.

Van Aken, J. 2004. Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules. Journal of Management Studies 41:2

Electronic references

Adams C. & Farrell S. 1999. Internet X.509 Public Key Infrastructure Certificate Management Protocols. Referenced 17.2.2012. http://www.ietf.org/rfc/rfc2510.txt

Bank for International Settlements. 2006. Basel Committee on Banking Supervision - Core Principles for Effective Banking Supervision. Referenced 10.10.2011 http://www.bis.org/publ/bcbs129.pdf

Cert-fi. TLS-protokollaa vastaan kehitetty BEAST-hyökkäys. Referenced 20.5.2012. http://www.cert.fi/tietoturvanyt/2011/09/ttn201109271116.html

Chokhani, S., Ford,W., Sabett, R., Merrill,C. & Wu,S. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. 2003. Referenced 21.11.2011. http://www.ietf.org/rfc/rfc3647.txt

Comodo incident report. 2011. Referenced 21.11.2011. http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

Coviello, A. 2011. Open Letter to RSA Customers. Referenced 31.10.2011 http://www.rsa.com/node.aspx?id=3872)

The Finnish bankers' association - Information security committee. 9.5.2001. PATU security functions for data transfer between customer and bank - part 1: procedures for authentication, integrity control and key management version 1.22. Referenced 16.2.2012. http://www.fkl.fi/en/material/publications/Publications/PATU_security_functions_for_data_transfer_between_customer_and_bank.pdf

European Payments Council. SEPA visions and goals. Referenced 16.2.2012. http://www.europeanpaymentscouncil.eu/content.cfm?page=sepa_vision_and_goals

Interim Report 2011. Investigation DigiNotar Certificate Authority Environment (http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf).

Lacey, D. 2011. Security: Best practice or ancient ritual? Referenced 31.1.2012. http://www.computerworlduk.com/in-depth/security/3256436/security-best-practice-or-ancient-ritual/#Scene_1

Microsoft Window Server TechNet Library. 2003. Designing a Public Key Infrastructure. Referenced 16.2.2012. http://technet.microsoft.com/en-us/library/cc773138(v=ws.10).aspx

Mobile certificate 2011. Referenced 31.10.2011. http://www.mobiilivarmenne.fi/en/index.html .

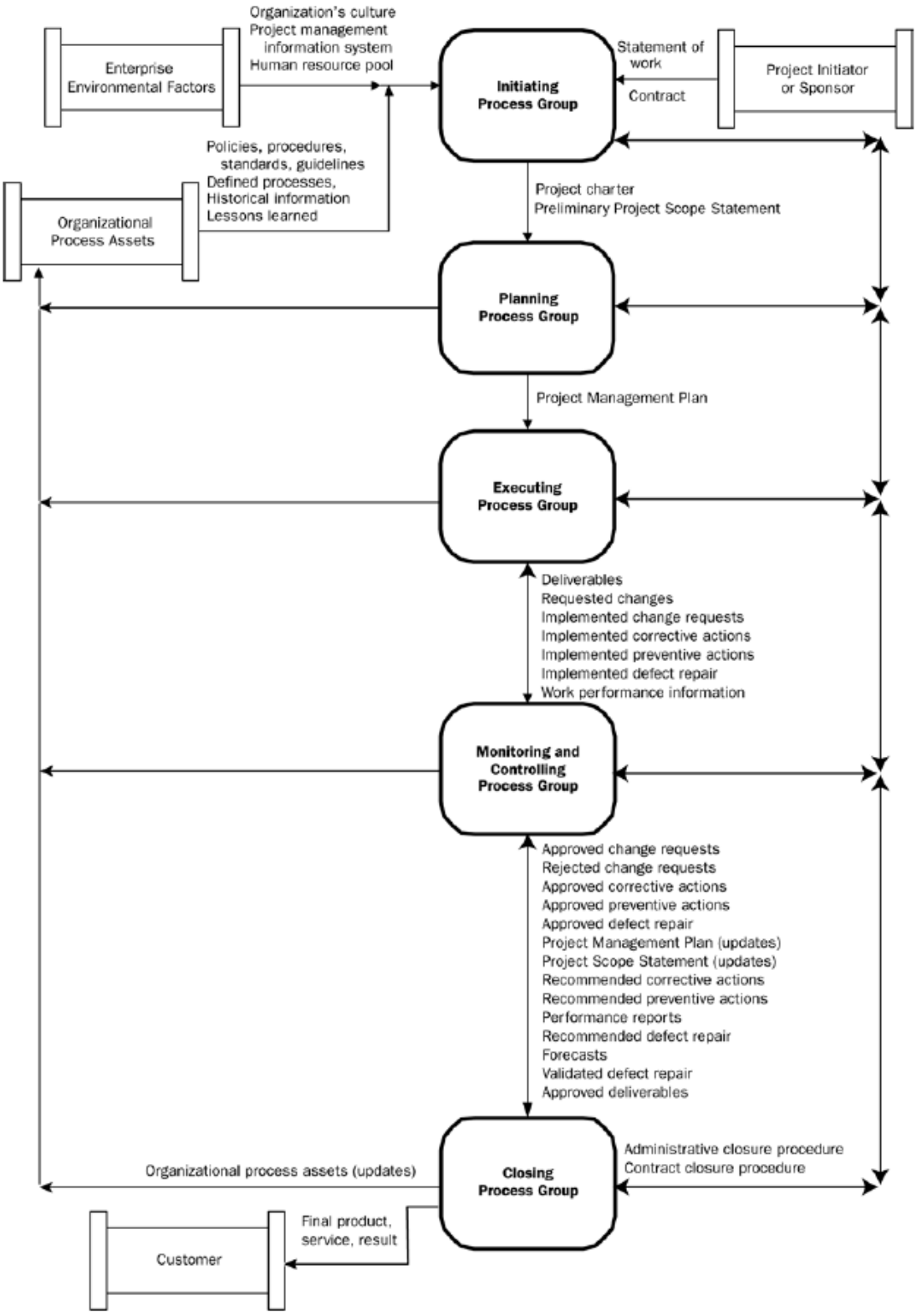
Nordea, OP-Pohjola Group, Sampo Bank 2008. Security and Message Specification for Financial Messages using Web Services. Version 1.05. Referenced 16.2.2012. http://www.fkl.fi/teemasivut/sepa/tekninen_dokumentaatio/Dokumentit/WebServices_Messages_20081022_105.pdf

Keizer, B. 2012.VeriSign Admits Multiple Hacks in 2010, Keeps Details Under Wraps. PC World. Referenced 9.4.2012. http://www.pcworld.com/businesscenter/article/249232/verisign_admits_multiple_hacks_in_2010_keeps_details_under_wraps.html

Figures

Appendix

Appendix 1 High lever summary of processes (PMBOK guide. 2004. 42)



Appendix 2 Key Management Inserts for Security Plan Templates (Barker, E., Barker, W., Burr ,W. & Polk ,W. and Smid, M. 2002.72)

1. Information System Name/Title

- Unique identifier and name given to the system.

2. Information System Categorization

- Identify the appropriate FIPS 199 categorization.

3. Information System Owner

- Name, title, agency, address, email address, and phone number of person who owns the system.

4. Authorizing Official

- Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

5. Other Designated Contacts

- List other key personnel, if applicable; include their title, address, email address, and phone number.

6. Assignment of Security Responsibility

- Name, title, address, email address, and phone number of person who is responsible for the security of the system.

7. Information System Operational Status

- Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

8. Information System Type

- Indicate if the system is a major application or a general support system.

9. General System Description/Purpose

- Describe the function or purpose of the system and the information processes.

10. System Environment

- Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.
- Key management-specific information that needs to be included in this section includes identification of any cryptographic mechanisms employed (including key variable sources) and the location of stored and archived cryptographic key variables.

11. System Interconnections/Information Sharing

- List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

12. Related Laws/Regulations/Policies

- List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

13. Minimum Security Controls

- Provide a thorough description of how the minimum controls in the applicable baseline are being implemented or planned to be implemented. The controls should be described by control family and indicate whether it is a system control, hybrid control, common control, scoping guidance is applied, or a compensating control is being used.

- Key management-specific information that needs to be included in this section includes: key archiving and recovery procedures in support of recovery of encrypted files; controls for validation of digital signature and other integrity keying materials (certification authority and controls for determining completeness/correctness); key management procedures for key generation, distribution, storage, and disposal; and applicable cryptographic standards and guidelines for all cryptographic mechanisms employed. This information may be included in a key management appendix.

14. Information System Security Plan Completion Date

- Enter the completion date of the plan.

15. Information System Security Plan Approval Date

- Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.

16. Key Management

1. Identification of the Keying Material Manager (The keying material manager **should** report directly to the organization's chief executive officer, chief operations executive, or chief information systems officer. The keying material manager is a key employee who **should** have been determined to have the capabilities and trustworthiness commensurate with responsibility for maintaining the authority and integrity of all formal electronic transactions and the confidentiality of all information that is sufficiently sensitive to warrant cryptographic protection.)

2. Identification of the management entity(ies) responsible for Certification Authority (CA) and Registration Authority (RA) functions and interactions. (Where applicable: where public key cryptography is employed, either the keying material manager or his/her immediate superior **should** be designated as the organization's manager responsible for Certification Authority and Registration Authority functions.)

3. Key Management Organization (Identification of job titles, roles, and/or individuals responsible for the following functions:)

a. Key generation or acquisition;

b. Agreements with partner organizations regarding cross certification of keying material;

c. Key distribution and revocation structure design and management,

d. Establishment of cryptoperiods;

e. Distribution of and accounting for keying material;

f. Protection of secret and private keys and related materials;

g. Emergency and routine revocation of keying material;

h. Auditing of keying material and related records;

i. Destruction of revoked or expired keys;

j. Key recovery;

k. Compromise recovery;

l. Contingency planning;

m. Disciplinary consequences for the willful or negligent mishandling of keying material; and

n. Generation, approval, and maintenance of key management practices statements.

4. Key Management Structure (Description of key certification, distribution and revocation trees for encryption, signature, and other cryptographic processes implemented within the organization. Description of procedures for modifying the trees and for establishing cryptoperiods.)

5. Key Management Procedures

a. Key Generation (Brief description of the procedures to be followed for key generation. This section includes reference to applicable standards and guidelines. Some procedures may be presented by reference. Note that not all organizations that employ cryptography will necessarily generate keying material.)

b. Key Acquisition (Identification of source(s) of keying material. Description of ordering procedures and examples of any forms employed in ordering keying material.)

c. Cross Certification Agreements (Description of cross certification procedures and examples of any forms employed in establishing and/or implementing cross certification agreements.)

d. Distribution of and Accounting for Keying Material (Description of procedures and forms associated with requests for keying material, acknowledgement and disposition of the requests, receipting for keying material, creating and maintaining keying material inventories, reporting destruction of keying material, and reporting acquisition or loss of keying material under exceptional circumstances.)

e. Emergency and Routine Revocation of Keying Material (Description of rules and procedures for the revocation of keying material under both routine and exceptional circumstances, such as notice of unauthorized access to operational keying material.)

f. Protection of Secret and Private Keys and Related Materials (Methods and procedures employed to protect keying material under various circumstances, such as pre-operational, operational, revoked.)

g. Destruction of Revoked or Expired keys (Procedures and guidelines identifying circumstances, responsibilities, and methods for destruction of keying material.)

h. Auditing of Keying Material and Related Records (Description of circumstances, responsibilities, and methods for auditing of keying material.)

i. Key Recovery (Specification of circumstances and process for authorizing key recovery and identification of guidelines and procedures for key recovery operations.)

j. Compromise Recovery (Procedures from exposure of sensitive keying material to unauthorized entities.)

k. Disciplinary Actions (Specification of consequences for willful or negligent mishandling of keying material.)

l. Change Procedures (Specification of procedures for effecting changes to key procedures.)

Appendix 3 PKI roles and actions - Microsoft server 2003. (Microsoft Window Server TechNet Library. 2003.)

PKI Roles

PKI Administrative Role	Description	Windows Server 2003 Administrative Role
PKI Administrator	Configures, maintains, and renews the CA.	User
Backup Operator	Performs system backup and recovery.	Backup Operator on the server on which the CA is running
Audit Manager	Configures, views, and maintains audit logs.	Local Administrator on the server on which the CA is running
Key Recovery Manager	Requests retrieval of a private key stored by the service.	User
Certificate Manager	Approves certificate enrollment and revocation requests.	User
User Manager	Manages users and their associated information.	Account Operators (or person delegated to create user accounts in Active Directory)
Enrollee	Requests certificates form the CA	Authenticated Users

PKI roles actions

Action	Enrollee	CA Admin	Certificate Manager	Audit Manager	Backup Operator	Local Server Admin
Install a CA						•
Configure a CA		•				•
Policy and exit module configuration		•				
Stop/start service		•				•
Change configuration		•				
Assign user roles		•				
Establish user accounts		•				•

Maintain user accounts		•				•
Configure profiles		•				•
Renew CA keys						•
Define key recovery agent(s)		•				
Define officer roles		•				
Enable role separation		•				
Issue/Approve certificates			•			
Deny certificates			•			
Revoke certificates			•			
Unrevoke certificates			•			
Renew certificates			•			
Enable, publish, or configure CRL schedule		•				
Configure audit parameters				•		•
Audit logs				•		•
Back up system					•	•
Restore system					•	•
Read CA properties, CRL	•					
Request certificate	•					
Read CA database		•	•	•	•	
Read CA configuration information		•	•	•	•	
Read issued, Revoked, pending certificates		•	•	•	•	

Appendix 4 Microsoft guidelines to design CA (Microsoft Window Server TechNet Library. 2003.)

- Do you require more than one CA? If you are only supporting a single application and location, and if 100 percent availability of the CA is not critical, you might be able to use a single CA. Otherwise, you probably require at least one root and multiple subordinate CAs.
- If you need more than one CA, how many root CAs do you require? Generally, it is recommended that you have only one root CA as a single point of trust. This is because significant cost and effort is required to protect a root CA from compromise. With multiple root CAs, root maintenance becomes much more difficult.
  However, organizations with a decentralized security administration model, such as corporations with multiple, largely independent business units and no strong central administrative body, might require more than one root CA.
- How many intermediate or policy CAs do you need?
- How many issuing CAs or RAs do you need?
  The number of intermediate and issuing CAs that you deploy depends on the following factors:
  - **Usage.** Certificates can be issued for a number of purposes (for example, secure e-mail, network authentication, and so on). Each of these uses might involve different issuing policies. Using separate CAs provides a basis for administering each policy separately.
  - **Organizational or geographic divisions.** You must have different policies for issuing certificates, depending on the role of an entity or its physical location in the organization. You can create separate subordinate CAs to administer these policies.
  - **Distribution of the certificate load.** You can deploy multiple issuing CAs to distribute the certificate load to meet site, network, and server requirements. For example, if network links between sites are slow or discontinuous, you might need to place issuing CAs at each site to meet Certificate Services performance and usability requirements.
  - **The need for flexible configuration.** You can tailor the CA environment (key strength, physical protection, protection against network attacks, and so on) to provide a balance between security and usability. For example, you can renew keys and certificates more frequently for the intermediate and issuing CAs that are at high risk for compromise, without requiring a change to established root trust relationships. Also, when you use more than one subordinate CA, you can turn off a subsection of the CA hierarchy without affecting established root trust relationships or the rest of the hierarchy.
  - **The need for redundant services.** If one enterprise CA fails, redundancy makes it possible for another issuing CA to provide users with uninterrupted service.

Appendix 5 Operational team actions

- Registering users
- Authorising and performing revocations
- Maintaining root keys of CAs and RAs
- Handling recovery from key loss
- Regularly checking operating system logs for signs of failure,
- Problems, or suspicious events
- Escalating suspicious events
- Dealing with technical queries on the PKI software
- Monitoring the performance of key servers
- Applying patches and bug-fixes
- Managing the file store and checking quotas
- Taking backups and holding these in a secure location
- Identifying potential problems and investigating them
- Liaising with PKI software vendors and other third parties
- Resolve issues
- Maintaining general secure services

Appendix 6 Public key infrastructure policy framework rfc3647 (Chokhani, S., Ford,W., Sabett, R., Merrill,C. & Wu,S. 2003.)

1. INTRODUCTION
1.1 Overview
1.2 Document name and identification
1.3 PKI participants
1.3.1 Certification authorities
1.3.2 Registration authorities
1.3.3 Subscribers
1.3.4 Relying parties
1.3.5 Other participants
1.4 Certificate usage
1.4.1. Appropriate certificate uses
1.4.2. Prohibited certificate uses
1.5 Policy administration
1.5.1 Organization administering the document
1.5.2 Contact person
1.5.3 Person determining CPS suitability for the policy
1.5.4 CPS approval procedures
1.6 Definitions and acronyms
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES
2.1 Repositories
2.2 Publication of certification information
2.3 Time or frequency of publication
2.4 Access controls on repositories
3. IDENTIFICATION AND AUTHENTICATION
3.1 Naming
3.1.1 Types of names
3.1.2 Need for names to be meaningful
3.1.3 Anonymity or pseudonymity of subscribers
3.1.4 Rules for interpreting various name forms
3.1.5 Uniqueness of names
3.1.6 Recognition, authentication, and role of trademarks
3.2 Initial identity validation
3.2.1 Method to prove possession of private key
3.2.2 Authentication of organization identity
3.2.3 Authentication of individual identity
3.2.4 Non-verified subscriber information
3.2.5 Validation of authority
3.2.6 Criteria for interoperation
3.3 Identification and authentication for re-key requests
3.3.1 Identification and authentication for routine re-key
3.3.2 Identification and authentication for re-key after revocation
3.4 Identification and authentication for revocation request
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS
4.1 Certificate Application
4.1.1 Who can submit a certificate application
4.1.2 Enrollment process and responsibilities
4.2 Certificate application processing
4.2.1 Performing identification and authentication functions
4.2.2 Approval or rejection of certificate applications
4.2.3 Time to process certificate applications
4.3 Certificate issuance
4.3.1 CA actions during certificate issuance
4.3.2 Notification to subscriber by the CA of issuance of certificate
4.4 Certificate acceptance
4.4.1 Conduct constituting certificate acceptance
4.4.2 Publication of the certificate by the CA
4.4.3 Notification of certificate issuance by the CA to other entities
4.5 Key pair and certificate usage
4.5.1 Subscriber private key and certificate usage
4.5.2 Relying party public key and certificate usage
4.6 Certificate renewal
4.6.1 Circumstance for certificate renewal
4.6.2 Who may request renewal
4.6.3 Processing certificate renewal requests
4.6.4 Notification of new certificate issuance to subscriber
4.6.5 Conduct constituting acceptance of a renewal certificate
4.6.6 Publication of the renewal certificate by the CA
4.6.7 Notification of certificate issuance by the CA to other entities
4.7 Certificate re-keys
4.7.1 Circumstance for certificate re-keys

4.7.2 Who may request certification of a new public key
4.7.3 Processing certificate re-keying requests
4.7.4 Notification of new certificate issuance to subscriber
4.7.5 Conduct constituting acceptance of a re-keyed certificate
4.7.6 Publication of the re-keyed certificate by the CA
4.7.7 Notification of certificate issuance by the CA to other entities
4.8 Certificate modification
4.8.1 Circumstance for certificate modification
4.8.2 Who may request certificate modification
4.8.3 Processing certificate modification requests
4.8.4 Notification of new certificate issuance to subscriber
4.8.5 Conduct constituting acceptance of modified certificate
4.8.6 Publication of the modified certificate by the CA
4.8.7 Notification of certificate issuance by the CA to other entities
4.9 Certificate revocation and suspension
4.9.1 Circumstances for revocation
4.9.2 Who can request revocation
4.9.3 Procedure for revocation request
4.9.4 Revocation request grace period
4.9.5 Time within which CA must process the revocation request
4.9.6 Revocation checking requirement for relying parties
4.9.7 CRL issuance frequency (if applicable)
4.9.8 Maximum latency for CRLs (if applicable)
4.9.9 On-line revocation/status checking availability
4.9.10 On-line revocation checking requirements
4.9.11 other forms of revocation advertisements available
4.9.12 Special requirements re key compromise
4.9.13 Circumstances for suspension
4.9.14 Who can request suspension
4.9.15 Procedure for suspension request
4.9.16 Limits on suspension period
4.10 Certificate status services
4.10.1 Operational characteristics
4.10.2 Service availability
4.10.3 Optional features
4.11 End of subscription
4.12 Key escrow and recovery
4.12.1 Key escrow and recovery policy and practices
4.12.2 Session key encapsulation and recovery policy and practices

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls
5.1.1 Site location and construction
5.1.2 Physical access
5.1.3 Power and air conditioning
5.1.4 Water exposures
5.1.5 Fire prevention and protection
5.1.6 Media storage
5.1.7 Waste disposal
5.1.8 Off-site backup
5.2 Procedural controls
5.2.1 Trusted roles
5.2.2 Number of persons required per task
5.2.3 Identification and authentication for each role
5.2.4 Roles requiring separation of duties
5.3 Personnel controls
5.3.1 Qualifications, experience, and clearance requirements
5.3.2 Background check procedures
5.3.3 Training requirements
5.3.4 Retraining frequency and requirements
5.3.5 Job rotation frequency and sequence
5.3.6 Sanctions for unauthorized actions
5.3.7 Independent contractor requirements
5.3.8 Documentation supplied to personnel
5.4 Audit logging procedures
5.4.1 Types of events recorded
5.4.2 Frequency of processing log
5.4.3 Retention period for audit log
5.4.4 Protection of audit log
5.4.5 Audit log backup procedures
5.4.6 Audit collection system (internal vs. external)
5.4.7 Notification to event-causing subject
5.4.8 Vulnerability assessments
5.5 Records archival
5.5.1 Types of records archived
5.5.2 Retention period for archive
5.5.3 Protection of archive
5.5.4 Archive backup procedures
5.5.5 Requirements for time-stamping of records
5.5.6 Archive collection system (internal or external)
5.5.7 Procedures to obtain and verify archive information
5.6 Key changeover

Appendix 7 Audit steps (The Information Systems Audit and Control Association & Foundation. 2001. 3)

A. Prior Audit/Examination Report Follow-Up

Review prior report and verify completion of any agreed-upon corrections. Note remaining deficiencies

B. Preliminary Audit Steps

Obtain:

-Organization chart

-Information architecture model for the organization

-Data classification policy

-Network infrastructure documentation

-Inventory of operating systems, applications, and operating systems impacting classified data

-Specifications of encryption tool(s)

-Understanding of external requirements (consider international encryption laws)

Obtain or perform risk assessment on the information need for encryption

Obtain infrastructure software acquisition procedures

Obtain maintenance history of all encryption tools in use

C. Detailed Audit Steps

Planning

Identify the security responsibilities within the organization.

Determine the level of involvement in the encryption processes by the security staff

Review the data requirements for encryption for the e-commerce environment

Review the regulatory requirements for encryption within the country, industry and organization and determine level of compliance

Determine level of risk existing considering the level of encryption implementation status.

Identify acceptable risk and determine if any residual risk exceeds the acceptable level

Review the decision process for selection of symmetrical (private key) usage

Review the tools selection process relative to compatibility with existing technologies

Acquisition, Implementation, Maintenance of Encryption

Review the acquisition process by which the encryption either has been or will be obtained, and determine validity to needs requirements

Review the implementation procedures for encryption tools

Determine access controls over keys during the acquisition/development process

Review the change control processes over infrastructure software (encryption tools)

Review the inventory of systems, applications and operating systems using (or to use) this encryption technique

Assess effectiveness of the encryption output compliance to external regulations and organizational policies

Key Management

Determine the access over keys is appropriate

Review the processes by which keys are/will be disseminated, maintained and cancelled

Review the key's expiration process

Miscellaneous

Review control around meta-data over keys, key management, encryption processes and related infrastructure resources

Appendix 8 PKI Questionnaire (The Information Systems Audit and Control Association & Foundation. 2001. 7)

General

Have all items from prior audits been cleared?
Is there an information architecture model that reflects current business needs?
Does the information architecture model support PKI data requirements?
Are sufficient policies in place and communicated to define data/information as an asset?

Either by policy or precedent, is information required to have the following characteristics:
- Efficiency?
- Effectiveness?
- Integrity?
- Availability?
- Confidentiality?
- Compliance?
- Reliability?

Is there a risk measure performed on an organizational need for encryption?
Has a concept of acceptable risk been adopted?
Is there a compliance "watch" function?
Does the current hardware infrastructure support the PKI plan?
Does the current software infrastructure support the PKI data requirements?
If the current infrastructure does not support the PKI plan, are there sufficient hardware and software planning initiatives that will provide the appropriate support to obtain the necessary tools and will not present unacceptable risk?

Planning

Is there an IT security function involved in security tool recommendations?

Are there detailed procedures for private key management?
Do they include:
- Generation?
- Dissemination?
- Implementation?
- Expiration?

Do the current or planned encryption tools work with existing infrastructure?

Acquisition, Implementation, Maintenance of Encryption

Do current tools meet all requirements?

Do all systems that require encryption use it?
Do infrastructure programs (encryption) follow established change control procedures?
Are encryption practices compliant with all applicable regulatory entities?

Key Management

Are appropriate controls in place over encryption keys?